INTEGRACJA SYSTEMÓW – JAK UZYSKAĆ KOMFORT ZAMIAST KOSZMARU

Integracja jako przedmiot projektu, a nie hasło

Dariusz OKRASA

W czasie wykładu zwrócono uwagę na następujące zagadnienia:

- Integracja jako przedmiot projektu, a nie hasło.
- Po co integrować?
- Co i jak integrować?

Kluczową kwestią jest przy tym precyzyjne określenie zakresu integracji, która powinna wynikać z rzeczywistych potrzeb. Możliwe jest stworzenie systemu, w którym wszystkie zintegrowane podsystemy w budynku podłączone są do jednego serwera centralnego i dostępne są dowolne interakcje pomiędzy wszystkimi urządzeniami takiego systemu. Jest to rozwiązanie bardzo kuszące w czasie przygotowywania inwestycji, bo jest proste logicznie i łatwe do opisania przy opracowywaniu wymagań. W praktyce takie systemy okazują się skomplikowane w eksploatacji, a stosunek ich funkcjonalności do ceny bardzo odbiega od rozwiązań optymalnych.

Słowo „integracja" pojawia się w wielu opisach i wymaganiach dotyczących elektronicznych systemów instalowanych w budynkach. Wymóg integracji dotyczy zazwyczaj nie tylko systemów automatyki budynkowej, ale także systemów przeciwpożarowych oraz systemów zabezpieczeń technicznych. Celem jest oczywiście ułatwienie bieżącej obsługi i raportowania, umożliwienie automatycznych działań wywoływanych przez określone zdarzenia oraz praca systemów według skonfigurowanych wcześniej scenariuszy i harmonogramów.

Najbardziej oczywistą strukturę systemu, prowadzącą do rozwiązania, w którym informacje ze wszystkich podsystemów są zbierane w jednym miejscu, a następnie i tak w większości rozdzielane według źródła ich pochodzenia, pokazano na rys. 1.

Systemy, które najczęściej podlegają integracji:

- System Sygnalizacji Włamania i Napadu (SSWiN) – ang. *Intrusion & Holdup Alarm System* (I&HAS),
- System Kontroli Dostępu (SKD) – ang. *Access Control System* (ACS),
- System Dozoru Wizyjnego (SDW) – ang. *Video Surveillance System* (VSS),
- System Automatyki Budynkowej (SAB) – ang. *Building Automation System* (BAS),
- Stałe Urządzenia Gaśnicze (SUG),
- System Automatyki Pożarowej (SAP).

Systemy zintegrowane mają następujące nazwy (wybór):

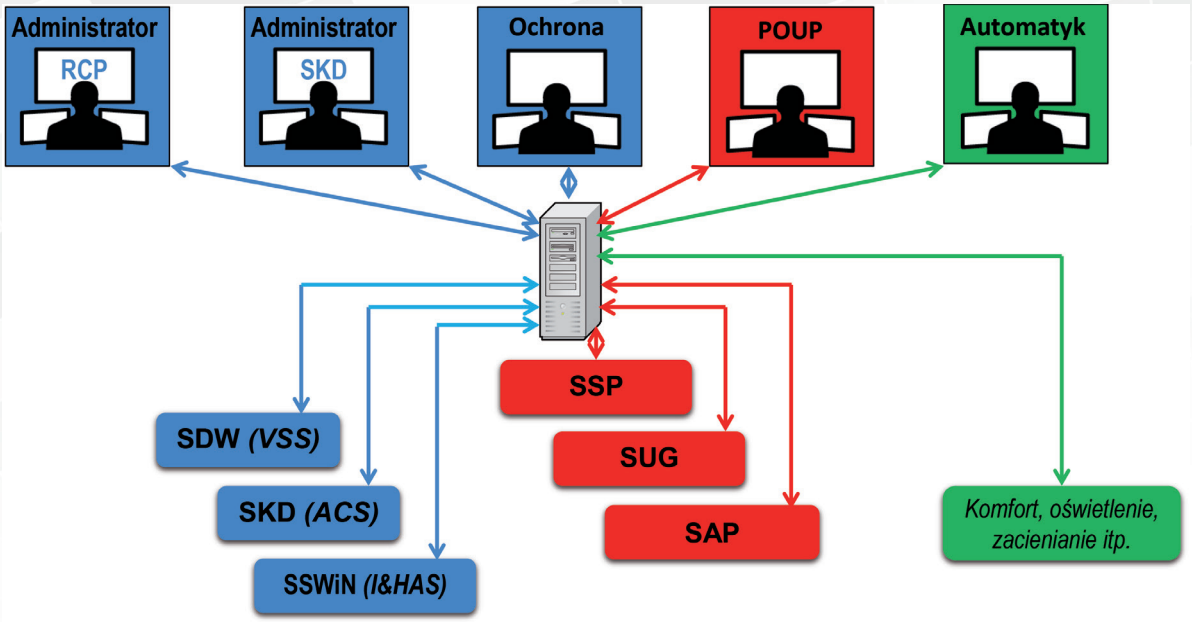
- Zarządzanie Informacją Bezpieczeństwa Fizycznego (ZIBF) – ang. *Physical Security Information Management* (PSIM),
- Zintegrowany System Zabezpieczeń (ZSZ) – ang. *Security Management System* (SMS),
- System Integracyjny Urządzeń Przeciwpożarowych (SIUP).

Inne skróty:

- **P**omieszczenie **O**bsługi **U**rządzeń **P**rzeciwpożarowych (**POUP**)

W celu prawidłowego ukierunkowania sposobu podejścia do integracji wystarczy zadać kilka pytań:

- Czy kiedykolwiek pracownikom ochrony będzie potrzebna informacja o temperaturze wody lodowej lub o konieczności wymiany filtrów powietrza nawiewanego do budynku?



Rys. 1. Uniwersalna struktura systemu zintegrowanego

- Czy kiedykolwiek w systemie sygnalizacji pożaru będzie wykorzystana informacja o stanie zapełnienia dysków rejestratora wizyjnego?
- Czy kiedykolwiek inżynierowi HVAC[1] będzie potrzebna informacja o uszkodzeniu ręcznego ostrzegacza pożarowego?

Odpowiedzi na te pytania są oczywiście przeczące. Po co w takim razie integrować? Bo można zadać też inne pytania:

- Czy w systemie automatyki może być wykorzystana informacja o wykryciu zagrożenia pożarowego?
- Czy w systemie ochrony przeciwpożarowej jest potrzebna informacja o zablokowaniu przejścia ewakuacyjnego?
- Czy pracownikowi ochrony będzie przydatna informacja o spadku temperatury poniżej zera wewnątrz budynku?

Odpowiedzi na te pytania są oczywiście twierdzące, co dowodzi, że integracja jest potrzebna. Kluczem do sukcesu jest zaprojektowanie integracji tak, aby dopasować ją do rzeczywistych potrzeb, zamiast integrować „wszystko ze wszystkim".

Projektowanie powinno rozpocząć się od przeprowadzenia **analizy funkcjonalnej** obiektu, która pozwoli na stworzenie wstępnej listy informacji (zakresu danych) istotnych dla działania innych podsystemów oraz koniecznych do wywołania zaplanowanych interakcji.

Następnym etapem jest opracowanie **wymagań użytkowych**, które będą zawierać:

- cel i funkcję wszystkich interakcji pomiędzy integrowanymi podsystemami,
- listę informacji wrażliwych, których udostępnianie musi być ograniczone lub niemożliwe,
- sposób działania i obsługa w przypadku awarii lub braku łączności/informacji,
- priorytety działania przy zdarzeniach masowych,
- sposób i czas przechowywania zarejestrowanych zdarzeń,
- procedury i sposób reakcji operatorów na zdarzenia,
- wymagania dotyczące testowania i konserwacji.

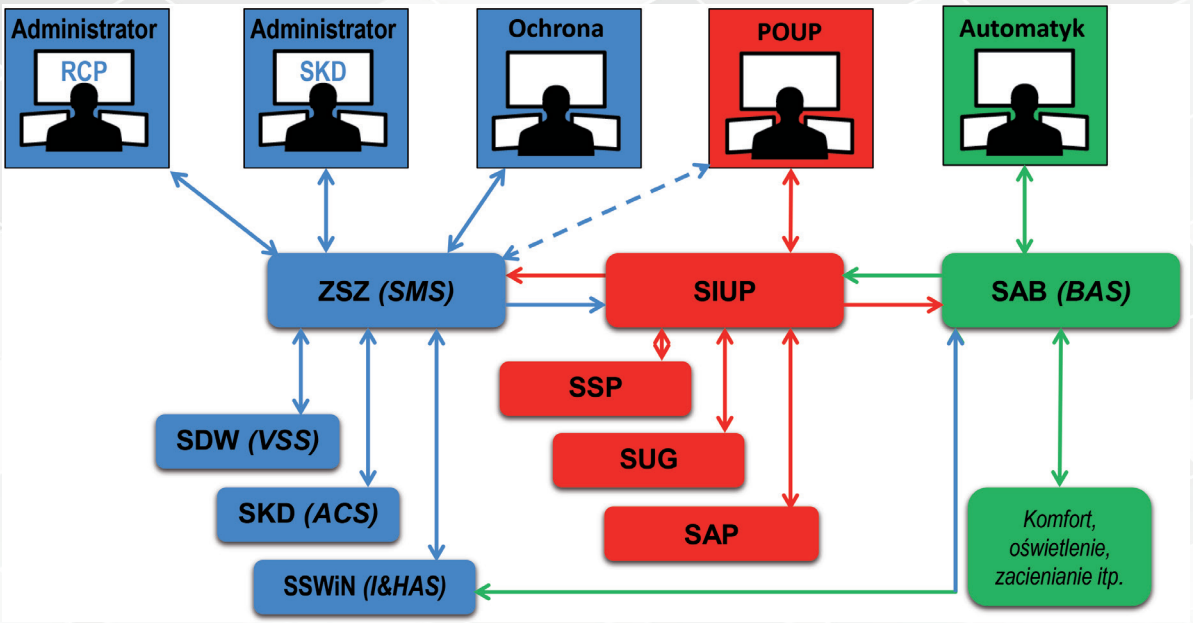
Dopiero na podstawie wymagań użytkowych można opracować **koncepcję**, zawierającą: opis sposobu obsługi, funkcje poszczególnych stacji operatorskich, algorytmy działań automatycznych, sposób wymiany poszczególnych informacji pomiędzy podsystemami oraz organizację i strukturę połączeń fizycznych i logicznych. W ramach wymagań użytkowych należy przeprowadzić także analizę ryzyka, istotną z uwagi na konieczność potwierdzenia, że każdy z podsystemów alarmowych będzie prawidłowo pełnił swoją funkcję jako część systemu zintegrowanego.

Końcowym krokiem jest **projekt techniczny**, wykonywany na podstawie koncepcji. Na tym etapie powinno być dobrane oprogramowanie i platforma sprzętowa urządzeń integrujących oraz sposobów wymiany informacji pomiędzy podsystemami, w tym: konkretne interfejsy, wspólne protokoły komunikacyjne, konwertery protokołów itp.

Przedstawiony wyżej sposób projektowania prowadzi najczęściej do struktury pokazanej na rys. 2., która różni się od uniwersalnego rozwiązania, pokazanego na rys. 1. Takie zoptymalizowane rozwiązanie jest zazwyczaj znacznie tańsze i łatwiejsze do wdrożenia z uwagi na ograniczoną liczbę problemów komunikacyjnych.

Podczas projektowania systemów zintegrowanych należy także pamiętać o wprowadzonej w ubiegłym

[1] HVAC (ang. *Heating, Ventilation, Air Conditioning*) – ogrzewanie, wentylacja, klimatyzacja.



Rys. 2. Zoptymalizowana struktura systemu zintegrowanego

roku Polskiej Normie PN-EN 50398-1:2017-10 (wersja angielska) *Systemy alarmowe. Systemy łączone i zintegrowane – Część 1: Wymagania ogólne.* Zgodnie z nazwą zawiera ona wymagania ogólne, ale także opisuje różne **Typy komunikacji** (1–4) oraz **Klasy centralnych urządzeń sterujących** (1–3) stosowane w celu integracji różnych systemów.

Najprostsza komunikacja, opisana w normie jako Typ 1., polega na jednokierunkowym przekazywaniu komunikatów lub sygnałów z jednego systemu do drugiego bez monitorowania łącza. Oznacza to, że nawet pojedyncze połączenie binarne, takie jak styki przekaźnika podłączone do wejścia bezpotencjałowego, jest traktowane przez normę jako integracja. Oczywiście kolejne typy komunikacji przewidują rozwiązania bardziej zaawansowane, aż do Typu 4., który zakłada szyfrowaną komunikację z potwierdzeniem i monitorowaniem integralności połączenia.

Centralne urządzenia sterujące służą do informowania obsługi o stanie systemu i mogą posiadać funkcje zarządzające i sterujące. Urządzenia najniższej Klasy 1. są przeznaczone do stosowania w tej samej lokalizacji, co urządzenia sterujące każdego z integrowanych systemów. Najwyższa, 3. Klasa, przeznaczona jest do stosowania w miejscach, gdzie nie są dostępne urządzenia sterujące wszystkich zintegrowanych systemów i wymagana jest redundancja. Dla każdej z klas norma określa wymagania dotyczące monitorowania pracy urządzeń i komunikacji, zasilania rezerwowego oraz redundancji i procedur postępowania w przypadku awarii.

Bardzo istotnym zapisem w tej normie jest wymóg, aby każdy z integrowanych systemów spełniał wymagania norm odpowiednich do poszczególnych systemów, a integracja nie może prowadzić do złagodzenia wymagań. Ponadto elementy wykorzystywane wspólnie przez kilka systemów powinny spełniać wymagania normatywne wszystkich wykorzystujących je systemów, a w przypadku różnic należy stosować wymagania najbardziej rygorystyczne.

Więcej szczegółów nt. integracji systemów przekazujemy w trakcie szkolenia organizowanego przez Ośrodek Szkoleniowy PISA: „Integracja systemów zabezpieczeń – uwarunkowania i procesy”.

Dariusz OKRASA

Od redakcji:
Absolwent Wydziału Elektroniki Politechniki Warszawskiej, od 1995 r. projektant systemów zabezpieczeń technicznych, ekspert Polskiej Izby Systemów Alarmowych, wykładowca Ośrodka Szkoleniowego PISA, członek Komitetu Technicznego Nr 52 Polskiego Komitetu Normalizacyjnego, Dyrektor Zarządzający w firmie ID Electronics. Specjalizuje się w kompleksowym zabezpieczaniu obiektów, a szczególnie w optymalizacji i wdrożeniach systemów sygnalizacji włamania i napadu, identyfikacji, kontroli dostępu oraz zagadnieniach wizualizacji i zarządzania systemami zintegrowanymi. Na wniosek Polskiej Izby Systemów Alarmowych odznaczony Srebrnym Krzyżem Zasługi i Medalem Komisji Edukacji Narodowej.