# KOMU POTRZEBNA JEST INTEGRACJA SYSTEMÓW ALARMOWYCH?


Cezary Mecwaldowski

Sergiusz Parszowski

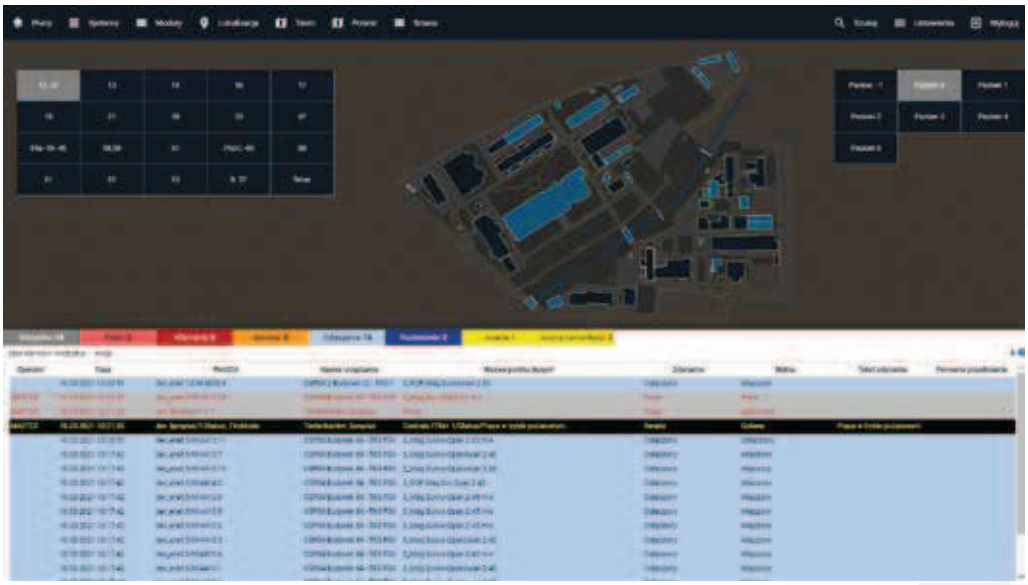

Jakie argumenty przemawiają za zastosowaniem integracji systemów zabezpieczeń elektronicznych? Dlaczego inwestor powinien podjąć decyzję o znacznych kosztach wdrożenia integracji? Poniższy artykuł spróbuje przybliżyć czytelnikowi odpowiedzi na postawione w tytule jak i we wstępie pytania. Przedstawione argumenty wykażą, że systemy integrujące, szczególnie kategorii PSIM (ang. Physical Security Information Management), są niezbędne w systemie zarządzania jakością i ciągłością działania firmy lub instytucji. Doświadczenie i analiza przypadków pozwala na wyodrębnienie kilku głównych czynników wpływających na decyzję inwestora o zastossowaniu systemu integrującego:

- Na etapie projektowania systemów, gdzie znana jest ich wielkość i liczba urządzeń, a także potrzeby funkcjonalne i cel stosowania. Systemy zintegrowane pozwalają uzyskać znacznie więcej funkcjonalności niż integrowane podsystemy i urządzenia.
- Na etapie istniejących systemów, kiedy koszt integracji jest odpowiednio proporcjonalny do integrowanych podsystemów i celu stosowania, wymagany jest wysoki poziom bezpieczeństwa obiektu.
- Na etapie istniejących systemów, kiedy liczba urządzeń i systemów sprawia trudności obsłudze (rozpoznanie zdarzenia, weryfikacja i reakcja) oraz nie pozwala na utrzymanie bieżącej sprawności systemów, wzrasta liczba usterek, napraw a inwestor traci poczucie posiadanego nadzoru nad urządzeniami i kosztami (rosną koszty eksploatacji).
- Na etapie istniejących systemów, kiedy pojawiają się trudności w efektywnej ich obsłudze przez użytkowników np. służbę ochrony, kiedy występują częste zmiany kadry, wiele lokalizacji i różnych systemów (co generuje potrzebę ujednolicenia obsługi i szkoleń, chociażby ze względu na możliwość zastępstw w ochronie obiektów).

Systemy integrujące posiadają wiele zalet i funkcjonalności, opisanych w literaturze[1], od obiektów cywilnych po struktury hierarchiczne w obiektach infrastruktury krytycznej[2]. W nawiązaniu do tematu artykułu, trzy z nich należy przywołać. Jedna to uproszczona i ujednolicona obsługa integrowanych, często bardzo zaawansowanych technicznie systemów, o skomplikowanych funkcjach np. automatyki pożarowej. Operator systemu zintegrowanego klika na zdarzenie pojawiające się w liście zdarzeń (stosie) widoczne na ekranie monitora (rys. 1), rozpoczynając procedurę obsługi zdarzenia. Zdarzenia mogą być generowane przez dziesiątki systemów i urządzeń, których znajomość obsługi byłaby wymagana bez zastosowania integracji. Jednak, gdy mamy integrację i stanowisko operatora, to na ekranie monitora pojawia się okno z krótką procedurą po-

[1] C.Mecwaldowski, *Integracja zabezpieczeń elektronicznych w zakładzie karnym*, OMiI, 4/2019.

[2] C.Mecwaldowski, *Zarządzanie rozproszoną infrastrukturą krytyczną na przykładzie obiektów Służby Więziennej*, AS Polska 5/2019.

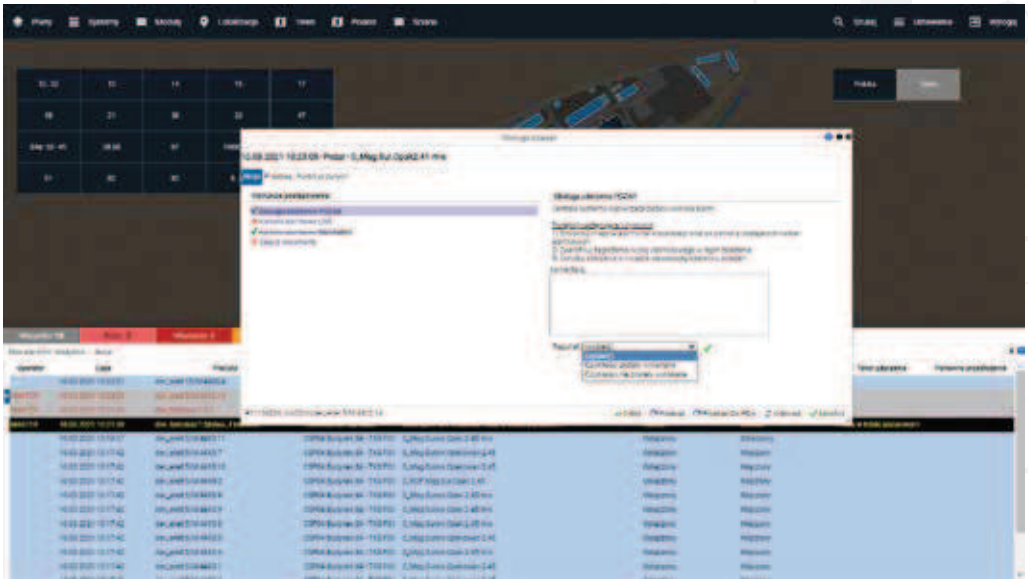


**Rys. 1.** Przykład stosu alarmowego – listy zdarzeń
*Źródło: Ela-compil*

stępowania, opcjami do wyboru (rys. 2). Zasada obsługi jest praktycznie identyczna i niezależna od systemów i urządzeń zintegrowanych. Operator jest w stanie szybko rozpoznać zdarzenie i zlokalizować na automatycznie wyświetlonej mapie obiektu ze wskazanym miejscem zdarzenia. Niezwykle ważną integracją, szczególnie w rozległych budynkach, czy obiektach z wieloma odległymi lokalizacjami jest powiązanie odpowiednich obrazów z kamer, z elementami integrowanych systemów oraz generowanymi przez nie sygnałami np. alarm z czujki ruchu powoduje automatyczne wyświetlenie obrazów z kamer z dozorowanego przez czujkę obszaru (rys. 3). Wszystko po to, aby operator mógł spróbować zdalnie zweryfikować i potwierdzić zdarzenie. Jeżeli weryfikacja zdalna nie może zostać zrealizowana, wtedy operator wysyła lub powiadamia-na wskazaną w procedurze osobę, grupę interwencyjną itp.

Drugą z ważnych cech systemu integrującego kategorii PSIM, o której należy wspomnieć to możliwość nadzoru infrastruktury, urządzeń aktywnych, na których platforma pracuje (w zakresie infrastruktury IT). Ponieważ większość obecnie stosowanych systemów i urządzeń posiada możliwości komunikacji w sieci Ethernet, systemy integrujące pozwalają skorzystać z dostępnych protokołów komunikacyjnych do nadzorowania urządzeń (rys. 4). Administrator systemu uzyskuje w ten sposób nadzór nad urządzeniami aktywnymi w sieci strukturalnej, łącznie z obciążeniem procesorów, dysków, ich temperaturą, strumieniami danych, stanem zasilania (zasilacze UPS) i wielu innych niezbędnych w danym rozwiązaniu informacji.

Trzecia cecha platformy integrującej, to jej moduły analityczne i raportujące. Funkcjonalność ta, to nie tylko raporty



**Rys. 2.** Przykład rozpoczęcia procedury obsługi zdarzenia przez operatora
*Źródło: Ela-compil*

**Rys. 3.** Przykład integracji zdarzenia z obrazem z kamer przy przejściu

**Rys. 4.** Przykład zarządzania infrastrukturą IT
*Źródło: Ela-compil*

tygodniowe, miesięczne, półroczne z funkcjonowania zintegrowanych systemów. To wykaz ilości zdarzeń alarmowych, technicznych, ale także informacje o funkcjonowaniu codziennym systemów i urządzeń np. dotyczących obciążenia przejść liczbą osób, pojazdów wjeżdżających na teren, wykorzystania szlabanów, wind, wentylacji, zadań wykonywanych przez użytkowników, służbę ochrony, a także samych operatorów systemu zintegrowanego (rys. 5). Raporty mogą być generowane dla osób odpowiedzialnych za ochronę obiektu, infrastrukturę techniczną czy obsługę finansową (rys. 6). Pozwalają oceniać efektywność i jakość wykonywanych konserwacji, napraw systemów. Dzięki temu inwestor może wybrać najlepszego usługodawcę. Zaskakująco często, przystępując do inwestycji w systemy bezpieczeństwa, nie bierze się pod uwagę kosztów eksploatacji. Najprawdopodobniej inwestor ulega przekonaniu, że bezpieczeństwo musi kosztować, nie jest to jednak podejście ani inżynierskie, ani jakościowe. Dobrym przykładem będzie przybliżona kalkulacja kosztów energii elektrycznej dla systemu telewizji dozorowej, w którym zainstalowano 400 kamer (ok 7,2 kW), 25 szt. switch-y (ok 0,4 kW), 2 szt. NVR (ok 0,5 kW), 4 monitory (ok 0,1 kW). Łączne obciążenie to ok. 8,2 kW, 197 kWh/dobę, 5910 kWh/miesiąc. Przy średniej cenie prądu 0,63 zł/kWh, miesięczny koszt energii pobieranej przez podany dla przykładu system to ponad 3 700 zł.

Kiedy po analizie ryzyka inwestor podejmie decyzję o wdrożeniu integracji systemów, przychodzi czas na ustalenia potrzeb w tym zakresie. Aby zrealizować wdrożenie i założenia integracji systemów alarmowych wraz z inną infrastrukturą techniczną budynków, niezbędne jest wprowadzenie następujących ról i podziału obowiązków. Inwestor wyznacza inspektora, który w jego imieniu i interesie będzie nadzorował cały proces integracji. Integrator to podmiot realizujący założoną integrację istniejących systemów i urządzeń. Zarówno inspektor jak i integrator powinni realizować swoje zadanie od początku do końca integracji. Związane jest to ze złożonością całego procesu, rozliczalnością. Osiągnięcie celu końcowego, czyli integracji podsystemów i urządzeń, przejęcie pełnej kontroli nad tysiącami urządzeń ma znacznie większe szanse powodzenia, kiedy inspektor oraz integrator prowadzą zadanie do końca. Doświadczenie to pokazuje. W procesie integracji uczestniczą jeszcze instalatorzy podsystemów i urządzeń, usługodawcy – konserwatorzy, firmy serwisujące. W tym

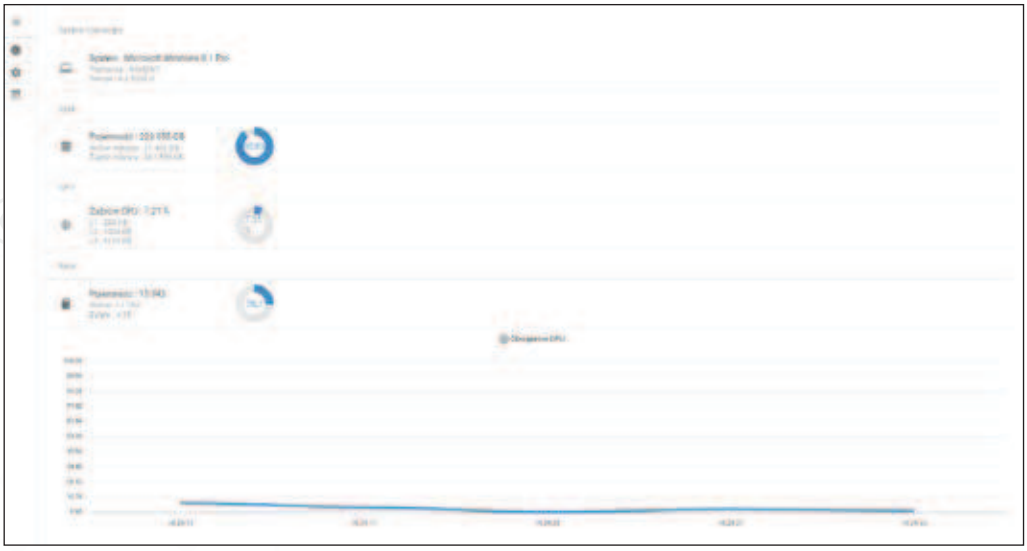
GEMOS
advanced PSIM

# Od 29 lat integrujemy systemy i aplikacje bezpieczeństwa w obiektach


ela.pl

facebook.com/
BuildingManagementSystems

linkedin.com/company/
elacompil



**Rys. 5.** Przykład modułu służącego do analizy zdarzeń
*Źródło: Ela-compil*

zakresie inwestor może dowolnie zmieniać uczestników na etapie integrowania. Z punktu widzenia inwestora, nie jest dobrze, kiedy integrator jest także instalatorem podsystemów i urządzeń. Jedną z ważniejszych zalet integracji jest to, iż pozwala szybko wskazać słabe punkty podsystemów i urządzeń np. awaryjność, złe wykonanie, zaprojektowanie (np. dobór detektorów). Kiedy integrator będzie jednocześnie wykonawcą takich podsystemów, może we własnym interesie, a wbrew interesom inwestora ukrywać wspomniane sytuacje.

Proces integracji bywa skomplikowany i wymaga czasu. Jednym z jego etapów jest weryfikowanie funkcjonalności i sprawności podsystemów. Wymaga to niejednokrotnie napraw lub zmian w podsystemach. Jednak efekt końcowy „ustabilizowania" systemów, czyli wyeliminowania usterek i błędów, uzyskanie rzeczywistego zarządzania systemami, rozliczalności działań usługodawców, użytkowników, operatorów (także w aspekcie finansowym) wpłynie bezpośrednio na podniesienie poziomu bezpieczeństwa w obiekcie.

**kpt. mgr inż. Cezary Mecwaldowski**
Wykładowca zakładu szkolenia ochronnego w Centralnym Ośrodku Szkolenia Służby Więziennej w Kulach.

**Sergiusz Parszowski**
Niezależny ekspert i doradca do spraw bezpieczeństwa i porządku publicznego. Audytor systemów bezpieczeństwa instytucji publicznych i podmiotów gospodarczych. Wykładowca akademicki oraz prelegent konferencji naukowych.

**Rys. 6.** Przykład modułu serwisowego
*Źródło: Ela-compil*