Security Management System

System wewnętrznie zintegrowany otwarty na inne systemy

Integracja systemów zabezpieczeń to aktualnie bardzo medialny temat. Prawie każdy chciałby mieć system zintegrowany, ale nie każdy wyobraża sobie, jak to powinno wyglądać. Nie jest łatwo w natłoku informacji marketingowych wybrać rozwiązanie najlepiej pasujące do potrzeb. Dlatego przedstawimy zasady integracji na przykładzie systemu zintegrowanego wewnętrznie, otwartego na integracje z innymi systemami – **INTEGRITI** australijskiej firmy **Inner Range**.

Gdy podchodzi się do tematu integracji, należy zastanowić się w pierwszej kolejności, jakie systemy chce się integrować i jak głęboko ta integracja ma przebiegać. Decyzję może ułatwić świadomość, jakie służby powinny należeć do obsługi obiektu wyposażonego w różne systemy budynkowe. W poważniejszych obiektach z reguły można wymienić minimum 4 stanowiska (rys. 1):

- obsługa systemów przeciwpożarowych, zlokalizowana w Pomieszczeniu Obsługi Urządzeń Przeciwpożarowych (POUP);
- administrowanie systemami zabezpieczeń technicznych (SZT), czasami z wydzielonym administrowaniem systemem kontroli dostępu,
- ochrona,
- obsługa systemów automatyki budynkowej.

Rys. 1. Podstawowe stanowiska służb odpowiedzialnych za różne systemy budynkowe

Na tej podstawie można podjąć logiczne decyzje, dotyczące tego, co z czym i jak głęboko integrować. Systemy powinny wymieniać między sobą informacje, ale pełna integracja po to, żeby następnie ją zdezintegrować, rozdzielając na przywołane wyżej 4 stanowiska, zwykle nie wydaje się uzasadniona. I do tego bardzo kosztowna, szczególnie integracja z systemami związanymi z ochroną przeciwpożarową. Dlatego większość integracji z systemami pożarowymi kończy się na wizualizacji i ewentualnie dostępie do kamer systemu dozoru wizyjnego w POUP oraz przyjmowaniu i wysyłaniu pojedynczych sygnałów między systemami. Analizując powyższe, można dojść do wniosku, że ścisła integracja jest wskazana dla systemów zabezpieczeń technicznych (SZT), natomiast powinna być możliwa, z reguły ograniczona do rzeczywistych potrzeb, współpraca z pozostałymi systemami budynkowymi. Przykładem może być współpraca SZT z automatyką budynkową, opisana bardziej szczegółowo w SEC&AS nr 6/2017[1].

Żeby lepiej zrozumieć problematykę integracji w specyfice systemów zabezpieczeń, należy zapoznać się z odrobiną teorii. W sposób popularny przedstawił ją dr inż. Marcin Buczaj z Wydziału Elektrotechniki i Informatyki Politechniki Lubelskiej[2]. Opisał m.in. jeden z ważniejszych podziałów, określających sposoby integracji systemów autonomicznych, a mianowicie „poprzez:

1. wymianę informacji między systemami autonomicznymi,
2. współdzielenie przez systemy elementów detekcyjnych i wykonawczych,
3. realizację funkcji przypisanych poszczególnym systemom przez ten sam układ sterujący”[3].

Nie decydując na tym etapie, który sposób integracji jest w danym momencie najkorzystniejszy, widać od razu, gdzie kryją się zagrożenia w przypadku systemów wskazanych w punktach 1 i 2 – oczywiście na styku pomiędzy urządzeniami lub systemami. Czyli jeżeli będą to systemy różnych producentów, to istnieje bardzo duże prawdopodobieństwo, często graniczące z pewnością, że systemy nie będą się dobrze „dogadywały”. Albo jeżeli dziś się dobrze „dogadują”, to po aktualizacji oprogramowania z reguły przestają. Problem ten rozwiązało stowarzyszenie Konnex, odpowiedzialne za standard KNX, dawniej nazywany EIB, nakazując certyfikację każdego urządzenia, które jest oznakowane logo KNX. Konnex jest chlubnym wyjątkiem na rynku, dlatego urządzenia z tym logo, produkowane przez różnych producentów, łączy się ze sobą bez problemów. Z innymi urządzeniami i systemami nie jest już tak różowo. Czyli można wygłosić niepopularne wśród inwestorów hasło, że bezpiecznie jest kupować rozwiązania jednego dostawcy, ponieważ jeżeli jest producentem markowym, to na pewno zadba, aby problemy się nie pojawiały, a nawet jak się pojawią, to bardzo szybko będą usunięte. Wyobraźmy sobie pozycję klienta, który kupił teoretycznie współpracujące ze sobą systemy różnych producentów, które, niestety, nie chcą współdziałać.

Na tym tle zerknijmy na systemy natywnie[4] wewnętrznie zintegrowane. Zintegrowane przez tego samego producenta, i do tego zintegrowane wewnętrznie. Z reguły nie trzeba w ogóle martwić się o taką integrację! Klient otrzymuje gotowe rozwiązanie i nie jest zmuszany do analizowania, co i jak ma ze sobą współpracować i czy w ogóle będzie ze sobą współpracowało, a jak coś trzeba będzie zmienić, to ile to będzie kosztowało. Czynnik ekonomiczny w eksploatacji systemów zintegrowanych okazuje się bardzo ważny. Niejeden inwestor jest zdruzgotany kosztami, jakie musi ponosić w trakcie eksploatacji, jeśli trzeba dokonać zmiany w systemie integrującym, korzystając z usług dostawcy. W systemach natywnie wewnętrznie zintegrowanych takie zmiany robią na bieżąco przeszkoleni administratorzy. Proszę sobie wyobrazić administratora zdalnie zarządzającego systemami zabezpieczeń w ponad 250 oddziałach jednego z polskich banków, który do każdej zmiany konfiguracji wzywałby serwis dostawcy!

Należy wyjaśnić również, co oznacza pojęcie „systemy heterogeniczne”. Otóż są to systemy niejednorodne, najczęściej pochodzące od różnych producentów. Integracja takich systemów jest możliwa, ale dużo trudniejsza ze względu na to, że systemy z reguły niejednorodne muszą się jakoś „dogadywać”. Producenci radzą sobie z tym problemem na różne sposoby, uzyskując lepsze lub gorsze rezultaty.

O ile oczywistym wydaje się to, iż oprogramowanie zarządzające jest zazwyczaj dobrze dopasowane do systemów zintegrowanych natywnie, o tyle system integrujący, np. typu SMS (ang. *Security Management System*), w przypadku systemów heterogenicznych może już tak optymalnie nie działać. Wówczas pozostaje jednoczesne stosowanie oprogramowania systemowego i oprogramowania integrującego. Nie jest to zarzut w stosunku do tego rozwiązania. Tak najczęściej po prostu jest i trzeba przyjąć tę informacje do wiadomości.

Mając już podstawową wiedzę na temat systemów natywnie wewnętrznie zintegrowanych można się zastanowić, jakie są najważniejsze cechy takiego rozwiązania. Przede wszystkim jest to najkorzystniejsze rozwiązanie w przypadku nowo wyposażanych obiektów (systemy są już fabrycznie zintegrowane, a więc nie trzeba ponosić dodatkowych kosztów na integrację).

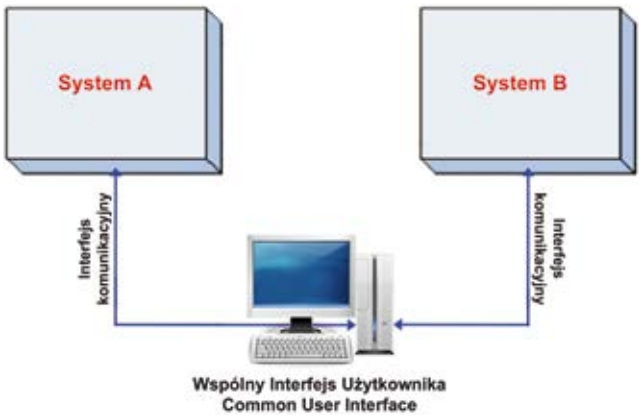
Systemy natywnie wewnętrznie zintegrowane są najkorzystniejszym rozwiązaniem w przypadku nowo wyposażanych obiektów.

[1] A. Tomczak: *Integracja systemu alarmowego z systemem inteligentnego budynku. Autentyczna potrzeba czy tylko moda?* SEC&AS, nr 6/2017, s. 36.

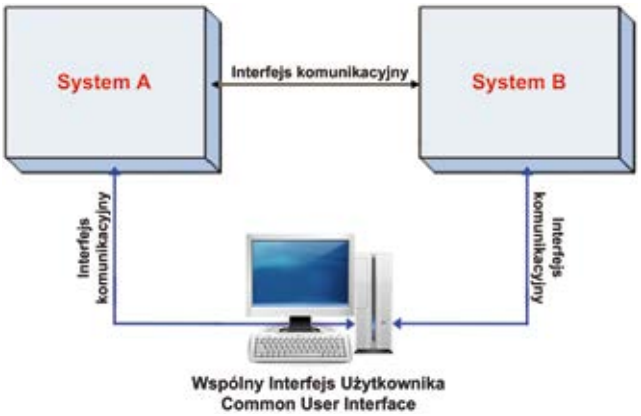
[2] Marcin Buczaj: *Integracja systemów alarmowych i systemów zarządzających pracą urządzeń w budynku mieszkalnym*. „Zabezpieczenia”, nr 4/2009.

[3] Ibidem.

[4] Natywny to inaczej wrodzony, rodzimy, co w technice oznacza, że został od początku np. zaprojektowany do danego działania.



Rys. 2. Klasa 1 – integracja systemów za pośrednictwem jednostki komputerowej

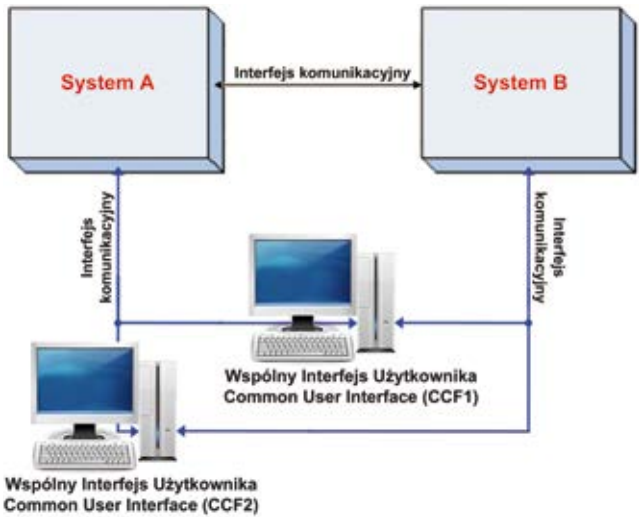


Rys. 3. Klasa 2 – redundantna integracja systemów za pośrednictwem jednostki komputerowej i bezpośrednio pomiędzy systemami

UWAGA: Taka konfiguracja może wskazywać na pełną integrację z wymianą sygnałów pomiędzy systemami, ale może również występować w przypadku monitorowania systemów i wspólnej wizualizacji.

Jest to rozwiązanie perspektywiczne, ponieważ w przypadku potrzeby zastosowania np. tylko jednego z podsystemów można bez przeszkód zrealizować jedynie okrojony system, a gdy w przyszłości trzeba będzie go rozbudować – nie będzie z tym problemu. W tym momencie może paść pytanie: a co z integracją dodatkowych systemów, np. heterogenicznych, czyli najczęściej pochodzących od innych producentów? To już zależy od polityki firmy, ale szanujący klienta dostawcy sprzętu otwierają się na systemy heterogeniczne.

Kolejny z podziałów sposobów integracji jest opisany w normie PN-EN 50398-1:2017-10 – *Systemy alarmowe. Systemy alarmowe łączone i zintegrowane. Część 1: Wymagania ogólne.* Norma podaje m.in. podział centrów nadzoru CCF (ang. *Central Control Facilities*) ze względu na poziom integracji oraz typ interfejsu i dzieli systemy na 3 klasy. Klasa 1, najniższa, dotyczy integracji systemów za pośrednictwem jednostki komputerowej (rys. 2).



Rys. 4. Klasa 3 – redundantna integracja systemów za pośrednictwem jednostki komputerowej i bezpośrednio pomiędzy systemami oraz redundantne centra nadzoru (CCF)

W przypadku integracji systemów zabezpieczeń norma dopuszcza takie rozwiązanie tylko warunkowo, a mianowicie wtedy, gdy w pomieszczeniu obsługi oprócz monitorów systemu komputerowego znajdują się klawiatury lub wyświetlacze stanów poszczególnych integrowanych systemów, z których obsługa może skorzystać w przypadku awarii urządzenia komputerowego. W klasie 2. oprócz komunikacji za pośrednictwem jednostki komputerowej musi być dodatkowo redundantnie zorganizowana komunikacja, pozwalająca na wymianę informacji, podobną jak w przypadku ścieżki wiodącej przez urządzenie komputerowe, tylko że bezpośrednio pomiędzy systemami (rys. 3). Wówczas dostęp do wszystkich standardowych interfejsów poszczególnych systemów nie jest wymagany, tak jak to było w przypadku klasy 1. W klasie 3. dodatkowo wymagana jest redundancja centrów nadzoru CCF (rys. 4).

Przywołana norma wprowadza również podział na cztery typy integracji, związane ze sposobem komunikacji pomiędzy poszczególnymi urządzeniami i systemami. W najwyższym, 4. typie integracji cała łączność pomiędzy urządzeniami i systemami jest szyfrowana (wszystkie sygnały sterujące, monitorujące i zwrotne) – rys. 5. W 3. typie integracji, przy pozostałych wymogach, tak jak w 4. typie, szyfrowanie całej komunikacji nie jest konieczne.

Jednakże np. w przypadku systemów kontroli dostępu norma PN-EN 60839-11-1[5] decyduje, kiedy szyfrowanie jest obowiązkowe. Przykładowo, obiekty infrastruktury krytycznej zostały przydzielone do 4. stopnia zabezpieczenia, w którym szyfrowanie jest obowiązkowe w miejscach, w których

[5] PN-EN 60839-11-2:2015-08 (wersja angielska): *Systemy alarmowe i elektroniczne systemy zabezpieczeń. Część 11-1: Elektroniczne systemy kontroli dostępu. Wymagania dotyczące systemów i części składowych.*

Rys. 5. Wymagania dla najwyższego typu integracji – typu 4

ZINTEGROWANY SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INTEGRITI

Systemy natywnie wewnętrznie zintegrowane w INTEGRITI firmy Inner Range:

- System Sygnalizacji Włamania i Napadu (SSWiN),
- System Kontroli Dostępu Osób i Pojazdów (SKD),
- Bezprzewodowe Systemy Kontroli Dostępu,
- System Dostępu do Wind,
- System Projektowania i Drukowania Identyfikatorów,
- System Obsługi Najemców (indywidualny dostęp najemcy do przydzielonego fragmentu bazy danych),
- System Obsługi Gości,
- Systemy Automatyki Budynkowej (BMS),
- System Obsługi Obiektów Rozproszonych.

Systemy heterogeniczne natywnie zintegrowane poprzez wymianę informacji między systemami autonomicznymi w INTEGRITI firmy Inner Range:

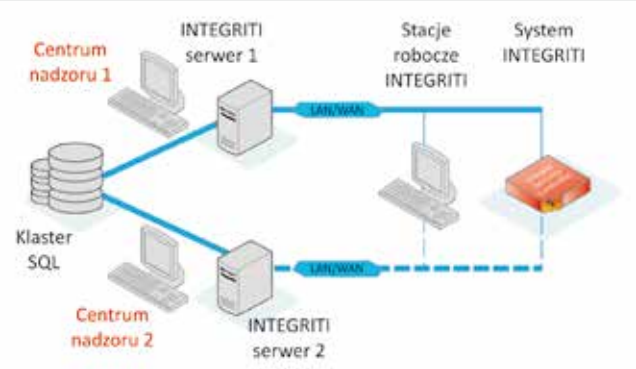
- Systemy Dozoru Wizyjnego (VSS),
- Systemy Zarządzania Wizją (VMS),
- Systemy Zarządzania Windami,
- Systemy Obsługi Gości,
- Systemy Automatyki Budynkowej (BMS),
- Systemy Depozytorów Kluczowych,
- Systemy Interkomowe,
- Systemy Sygnalizacji Pożaru,
- Systemy Kadrowe i Płacowe,
- Systemy Rozpoznawania Tablic Rejestracyjnych (ANPR),
- Systemy Ochrony Ogrodzeń.

Dostępne w INTEGRITI klasy centrów nadzoru (CCF):

Klasa 1 – integracja systemów za pośrednictwem jednostki komputerowej,

Klasa 2 – redundantna integracja systemów za pośrednictwem jednostki komputerowej i bezpośrednio pomiędzy systemami,

Klasa 3 – redundantna integracja systemów za pośrednictwem jednostki komputerowej i bezpośrednio pomiędzy systemami oraz redundantne centra nadzoru CCF (rys. 6).



Rys. 6. Redundantne zabezpieczenie centrów nadzoru w INTEGRITI

System INTEGRITI może być zrealizowany, w zależności od potrzeb klienta, w 3. lub 4. typie integracji, tzn. że można wprowadzić nie tylko pełne szyfrowanie całego systemu kontroli dostępu (rys. 7), co jest wymagane zarówno w 3., jak i 4. stopniu zabezpieczenia, np. dla obiektów infrastruktury krytycznej wg PN-EN 60839-11-1, ale również systemu sygnalizacji włamania i napadu (AES 128 bit), co jest unikalną cechą INTEGRITI.

Rys. 7. Pełne szyfrowanie całego systemu kontroli dostępu w INTEGRITI – 4. stopień zabezpieczenia wg PN-EN 60839-11-1

UWAGA 1: Ważna informacja dla użytkowników systemów kontroli dostępu opartych na kontrolerach GRANTA – **INTEGRITI zostało wyposażone w możliwość zarządzania istniejącymi systemami GRANTA**, bez potrzeby dokonywania jakichkolwiek zmian sprzętowych wewnątrz istniejących systemów.

UWAGA 2: Ważna informacja dla użytkowników systemów Inner Range starszej generacji, np. Concept 3000/4000 – **INTEGRITI jest kompatybilne wstecznie** i możliwe jest wdrożenie procesu migracji z istniejącego systemu Concept do INTEGRITI (takie operacje w Polsce już się odbyły). Konieczne zmiany dotyczą wyłącznie płyt głównych central (pozostałe infrastruktura pozostaje bez zmian) oraz oprogramowania zarządzającego bezpieczeństwem.

UWAGA 3: Dziesiątki firm w Polsce wykonywało instalację systemów Concept firmy Inner Range. Te same firmy mogą teraz wykonywać instalacje INTEGRITI lub migrację z systemów Concept do INTEGRITI.

komunikacja może być dostępna dla potencjalnego intruza, np. pomiędzy centralą a czytnikiem oraz kartą (nie mówiąc o samej karcie, w której nie wolno korzystać z niezakodowanych informacji, np. numeru UID/CSN[6]).

Tak w największym skrócie można streścić wybrane wątki dotyczące trudnej decyzji, na jaki sposób integracji najkorzystniej będzie się zdecydować, analizując konkretny obiekt, który ma podlegać zabezpieczeniu. Zainteresowanych pogłębieniem tej tematyki odsyłamy do wysłuchania kursu teoretycznego Integracja Systemów Zabezpieczeń, prowadzonego przez Ośrodek Szkoleniowy PISA.

[6] Zob. A. Tomczak: *Zwrot w podejściu producentów do systemów kontroli dostępu. Czyżby rewolucja na rynku SKD?*. SEC&AS, nr 4/2017, s. 21.

Artykuł firmy
ID Electronics Sp. z o.o.