BEZPIECZEŃSTWO POŻAROWE W ŚWIETLE DEFINICJI INTELIGENTNEGO BUDYNKU

Sławomir Bałuszyński*

ABSTRACT

One of the main reasons for the creation of an intelligent building was the desire to increase the sense of the safety of it users and it appeared in the USA in the early 80-s years of last century. At that time very fashionable and was rather of a commercial nature. In accordance with this trend people began to require contractors equipment facilities in modern systems technical infrastructure. The rapid development of information technology , electronics and automatic control systems has enabled the creation of building, which reacts automatically on the danger include the fire risk and thanks to the advanced technologies can quickly and effectively respond to changing situations in the indoors and its surroundings. There is also a new definition of the intelligent building who, in her notation account the users of the building, their needs and requirements[1] Nowadays inteligent buildings are class on the basis of a set of elements that differ in particular countries. The emphasis may be plased on "automation" functions,the appriopriate construktion-function solutions, friendly instlations, economic efficiency of a builging or the needs of users.

Key words:
security, risk, fire automation, fire systems

1 BEZPIECZEŃSTWO POŻAROWE W ODNIESIENIU DO DYREKTYW UNII EUROPEJSKIEJ

Należy podkreślić, że nie we wszystkich Państwach Członkowskich, a także nie we wszystkich działających w nich hotelach istnieją zasady bezpieczeństwa pożarowego a nawet tam gdzie istnieją, bywają niekompletne i niejednoznacznie, co z pewnością utrudnia otrzymanie przejrzystego obrazu bezpieczeństwa pożarowego[2].

W związku z gwałtownym rozwojem turystyki i podróży służbowych coraz więcej ludzi przebywa w hotelach Państw Członkowskich, różniących się od hoteli ich krajów pochodzenia. Niewatpliwie, osoby te mają prawo do odpowiedniej ochrony w goszczącym ich kraju ,oraz informacji o naturze i zakresie tej ochrony.

* mgr inż. Sławomir Bałuszyński- oficer pożarnictwa, członek European Association for Security

I chociaż dopuszcza się do pewnych różnic w typie lub konstrukcji hoteli w Państwach Członkowskich, można jednak ustalić minimalne standardy bezpieczeństwa pożarowego dla wszystkich hoteli a ich dostosowanie się do tego minimalnego standardu jest niezwykle istotne dla ich dalszej działalności. Z punktu widzenia zabezpieczenia przeciwpożarowego na poziomie Wspólnoty nie istnieją ujednolicone przepisy dotyczące używania i stosowania materiałów przeciwpożarowych. Jednak biorac pod uwagę powody ekonomiczne, bezpieczeństwo turystów i osób podróżujących z jednego Państwa Członkowskiego do drugiego, jest ważnym, aby promować obieg i rozpowszechnianie informacji na temat działań, chroniących hotele przed ryzykiem pożaru i dostosowanych do warunków danego kraju Do opracowywania i rozpowszechniania tego typu informacji została powołana specjalna, pełniąca w tej dziedzinie kluczową rolę Komisja, która zaleciła przedsięwziąć wszelkie dostępne środki w celu oparcia zabezpieczeń przeciwpożarowych w istniejących hotelach na zasadach wymienionych poniżej [3]:

- zmniejszenie ryzyka wybuchu pożaru,
- zapobieżenie rozprzestrzenianiu się ognia i dymu,
- zapewnienie bezpiecznej ewakuacji wszystkich obecnych w hotelu osób,
- umożliwienie podjęcia akcji służbom ratowniczym.

2 INTELIGENTNY BUDYNEK A AUTOMATYKA BUDYNKOWA

2.1 CHARAKTERYSTYKA BUDYNKÓW INTELIGENTNYCH

W krajach rozwiniętych technologicznie panuje powszechna opinia, że przyszłością przemysłu budowlanego jest budynek inteligentny. Budynki hotelowe to obiekty, w których inteligencja budynkowa jest wprowadzana najintensywniej. Rosnąca liczba hoteli na całym świecie jest przedstawiana przez właścicieli i administratorów jako budynki inteligentne. Rosnąca liczba budynków inteligentnych jest tłumaczona zataczającym coraz szersze kręgi przekonaniem, że inwestycja w „inteligencję budynkową" jest gwarancją uzyskania wymiernych korzyści, wśród których można wymienić[3]:

• redukcje kosztów eksploatacyjnych i użytkowania przestrzeni budynku;

• otrzymanie środowiska zbudowanego zaawansowanego technologicznie, które jest elastyczne,łatwe w obsłudze i wygodne dla użytkowników

• połączenie podniesienia jakości i technologicznego zaawansowania budynku z obniżeniem kosztów w odniesieniu do porównywalnego, tradycyjnego budynku;

• podniesienie efektywności, sprawności i atrakcyjności rynkowej obiektu.

2.2 OCZEKIWANIA W STOSUNKU DO BUDYNKÓW

Oczekiwania co do **inteligentnych funkcji budynków** [4] są różne i nie zawsze racjonalne, co wynika generalnie z wielkości i przeznaczenia samej budowli:

▪ *właściciel posesji z jednorodzinnym budynkiem* chce mieć zapewniony pełny komfort użytkownika czyli ergonomię, bezpieczeństwo i łatwość użytkowania, chce zapewnić sobie i domowi bezpieczeństwo poprzez kontrolę zamknięcia wszystkich otworów przed wyjściem, symulację obecności, wykrywanie i lokalizację intruz a wraz z alarmowaniem. Oczekuje łatwości sterowania i możliwości zmiany wybranych parametrów i funkcji (np. sterowanie wybranymi czynnościami spoza domu za pomocą komórki, wykorzystanie swego laptopa do wprowadzania zmian itp.), nie zawsze potrafi pogodzić się z oddaniem „pełnej władzy nad mediami domowymi" w ręce systemu (czyli jego zewnętrznej, obcej, wykwalifikowanej obsługi) – pragnie sam mieć „coś do powiedzenia" i to w sposób jemu znany i dla niego wygodny (np. żaluzje okienne przysłaniające słońce);

▪ *właściciel budynku mieszkalnego wielokondygnacyjnego/hotelu* chce z reguły automatyzować czynności ogólnie powtarzalne, zminimalizować koszty stałe (oświetlenie klatek schodowych, wind, pomieszczeń wspólnego użytkowania – garaże, piwnice), chce uproszczenia i obniżenia kosztów w zakresie dostarczania i wykorzystywania mediów (woda, ciepło, telekomunikacja itp.). Z zasady musi zrealizować funkcje zabezpieczenia ppoż. i ochrony fizycznej oraz zapewnić dostępność do wybranych innych funkcji i usług, przy zachowaniu pełnego nadzoru nad ich realizacją;

▪ *właściciel wielokondygnacyjnego biurowca,* wypożyczając w nim lokale musi liczyć się z różnymi wymaganiami swoich klientów, ale na pewno powinien standardowo uwzględniać komfort pracy w pomie-szczeniach (oświetlenie, klimatyzacja, ogrzewanie), dostępność mediów (sieci telekomunikacyjne i informatyczne) określone zabezpieczenia techniczne Zatem biorąc pod uwagę maksimum realizowanych odrębnych funkcji (elementarnych co do zidentyfikowanych atrybutów) powinniśmy analizować wszystkie powiązania potrzeb/oczekiwań i możliwości realizacyjne stanowiące o „inteligencji" budynku.

System Automatyki Budynkowej – BMS (*Building Management System*) jest „mózgiem" Inteligentnego Budynku [5].Integracja systemów stwarza ogromne możliwości zarządzania zasobami budynku, stanowiąc jednocześnie kluczowe zagadnienie – współcześnie „inteligencja" budynku kryje się w zintegrowanym systemie, wychodzącym naprzeciw potrzeb użytkownika przez elastyczną platformę współpracy różnorodnych (co do swej struktury i przeznaczenia) systemów teleinformatycznych i telekomunikacyjnych.

Głównymi elementami struktury pod względem bezpieczeństwa i ochrony (w rozumieniu zapewnienia ochrony wnętrza obiektu jak i nadzoru jego bezpośredniego otoczenia) są:

- kontrola dostępu (KD)
- system sygnalizacji włamania i napadu (SSWiN)
- system rejestracji czasu pracy (RCP)
- system nadzoru telewizyjnego (CCTV – *Close Circuit Television*)
- ochrona przeciwpożarowa – system alarmu pożarowego (SAP)
- autonomiczny system pożarowy (SP oraz SUG) i system nagłośnienia

alarmowego
- ogrzewanie, wentylacja i klimatyzacja
- system monitoringu parametrów środowiska
- system zarządzania energią (oświetleniem i windami).

BMS w rozumieniu stosowanych obecnie rozwiązań to integracja systemów z aktywnym sterowaniem poprzez komputer w układzie współzależnym łączone są działania systemów zamkniętych (np. bezpieczeństwa pożarowego) i otwartych (np. monitoring parametrów otoczenia)] przy zachowaniu warunku możliwości bezpośredniej ingerencji człowieka nadzorującego stan bezpieczeństwa budynku[6].

Rozwój systemów bezpieczeństwa w warunkach BMS związany jest nie tylko z zmianami technologicznymi (systemy EIB, LonWorks, BACnet), ale wynika z wdrażania nowego podejścia do rozwiązań zarządczych w samych systemach (system roju, systemy rozproszone, sieci neuronowe).

2.3 FUNKCJONOWANIE SYSTEMU

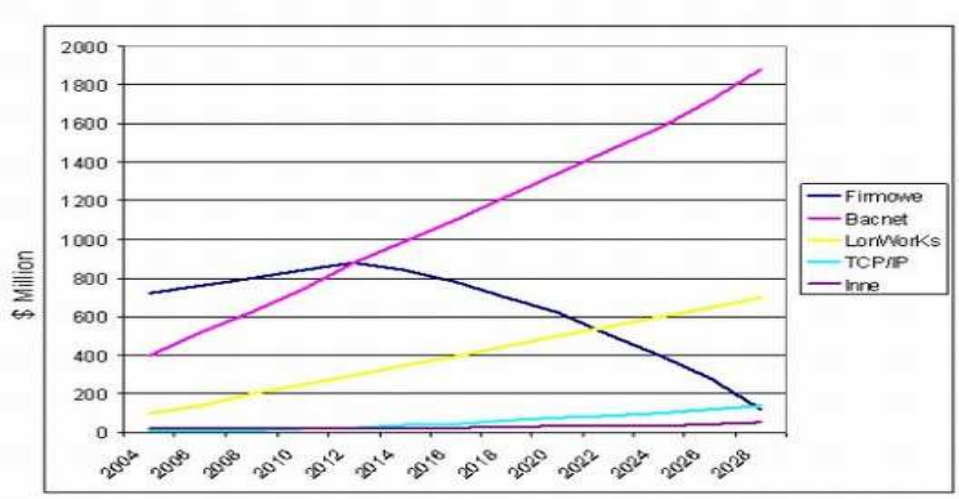
Pierwotne założenia „inteligentnego" budynku obejmowały wyłącznie instalacje alarmowe, oświetlenie i klimatyzację. Rewolucja w telekomunikacji i informatyce, zmiana standardów pracy biurowej spowodowały, że do budynków wdarły się sieci komputerowe, nowoczesne systemy automatyki i zabezpieczeń. Dziś systemy tworzące w strukturę „inteligentnego" budynku to m.in. ogrzewanie, wentylacja i klimatyzacja, oświetlenie, sieć telefoniczna i sieć komputerowa, system sygnalizacji pożaru, gaszenia i oddymiania, system sygnalizacji włamania i napadu, system nadzoru wizyjnego, system kontroli dostępu, system nagłośnieniowy, sieć elektroenergetyczna, sieć telewizji kablowej, satelitarnej i z nadajników naziemnych, system kontroli pracy strażników, sterowanie windami, żaluzje, szlabany itp. Zaczęto stosować również okablowanie strukturalne, cechujące się dużą uniwersalnością oraz łatwością dostosowania do zmieniających się potrzeb użytkownika i funkcji pomieszczeń. Można dzięki temu układać okablowanie bez wcześniejszej znajomości jakie urządzenia będą z niego korzystać[7] .

Oprócz wspomnianej wcześniej decentralizacji systemów sterowania obecnie widoczna jest również tendencja integracji podsystemów w jedną spójną całość. Integracja systemów stwarza ogromne możliwości, jeśli chodzi o zarządzanie zasobami budynku i jest to nieodłączny element samej idei inteligentnego budynku. To właśnie inteligencja budynku kryje się w zintegrowanym systemie, a realizacja takiego podejścia procentuje stworzeniem elastycznej platformy, która daje się łatwo adaptować, wychodząc naprzeciw potrzebom użytkownika.

Systemy automatyzacji budynku: BCS, EMS i BMS dla dowolnie dużego obiektu powinny być ze sobą zintegrowane w jeden system kontroli i zarządzania budynkiem (BMCS). Założenie takie w praktyce oznacza stosowanie nowoczesnych technologii, zarówno komputerów, sterowników, urządzeń peryferyjnych, jak i samych sieci komunikacyjnych wraz z protokołami komunikacyjnymi[8]. Od wyboru

właściwego systemu informatycznego zależy efektywność działania automatyki budynku. Zintegrowanie hardware'u i software'u różnych systemów i podsystemów to rozwiązanie, które zapewnia optymalna funkcjonalność automatyzacji budynku. Zatem system BMCS obejmuje sprzęt i aparaturę przyłączona do sieci, jak również systemy komunikacyjne, które umożliwiają dostęp do danych całego budynku czy kompleksu budynków. Dzięki integracji systemów użytkownik ma pełna informację o budynku i może zarządzać wszystkimi parametrami w budynku[9].

Obecnie, obserwuje się ekspansję w inteligentnych budynkach różnego rodzaju instalacji zapewniających szybką i bezpieczną wymianę informacji. Pojawia się potrzeba zapewnienia pracownikom sprawnej komunikacji ze światem zewnętrznym, przy wykorzystaniu różnych dróg transmisji. Zarówno Internet, jak i cyfrowa sieć ISDN umożliwiająca integrację różnych usług (przesyłanie danych, mowy, obrazu) są odpowiedzią na potrzebę jeszcze większego dostępu do informacji. Wraz z wdrażaniem nowoczesnych technologii pojawiają się również nowe problemy. W przypadku dostępu do Internetu, ważna jest ochrona danych przed dostępem osób do tego niepowołanych. Innym problemem jest zapewnienie tajności informacji przesyłanych pocztą elektroniczną. Biorąc pod uwagę fakt, że ten rodzaj komunikacji staje się coraz bardziej popularny, niezbędne jest stosowanie wielu poziomów zabezpieczeń[10]. Kolejnym zagadnieniem jest ochrona danych i przepływ danych wewnątrz budynku. W zależności od tego czy budynek zajmuje jedna organizacja, czy kilka, sieci telekomunikacyjne muszą być odpowiednio zorganizowane, ponieważ w interesie każdej firmy leży ochrona ich danych. Nowoczesny styl pracy wymaga m.in. sprawnej wymiany informacji, która może być przesyłana w różnej postaci (poczta elektroniczna, wideokonferencje). Dlatego inteligentny budynek, zgodnie z ideą, musi wciąż podążać za wciąż pojawiającymi się nowinkami technicznymi i zmieniającymi się potrzebami użytkowników. Poza bezpieczeństwem przesyłanych informacji, ważna jest ochrona budynku, szczególnie gdy mamy do czynienia ze zorganizowaną przestępczością. Nowoczesne systemy alarmowe wykorzystujące setki rodzajów zabezpieczeń muszą stawić czoła doskonale wyposażonym i coraz lepiej przygotowanym intruzom. Również pod tym względem rzeczywistość wymusza na inteligentnych budynkach stosowanie najnowocześniejszych rozwiązań[11].



Rys.1.Przewidywane trendy rozwoju poszczególnych standardów automatyki budynkowej do roku 2028 (źródło: Conference Dual Sourcing Vs. Sole Sourcing for Building Automation Controls, Washington, November 2005)

3. BEZPIECZEŃSTWO POŻAROWE, KOMFORT FIZYCZNY ORAZ BEZPIECZEŃSTWO BI DLA BUDYNKÓW INTELIGENTNYCH

Przez komfort fizyczny BI można rozumieć komfort cieplny, odpowiednią jakość powietrza wewnątrz BI (czyli jego wilgotność, prędkość, czystość i zawartość CO2) oraz prawidłowe oświetlenie. Z tych parametrów zdefiniowany jest zgodnie z normą PN-83/B-03430 tylko komfort cieplny jako stan, w którym człowiek jest zadowolony ze swojego termicznego otoczenia, czyli nie odczuwa ani zimna, ani gorąca [12]. Z parametrów komfortu fizycznego bardzo ważne są oświetlenie o odpowiednim natężeniu i dostęp do światła dziennego. Za utrzymanie sprzyjającego klimatu cieplnego wewnątrz BI odpowiadają systemy wentylacji, ogrzewania i klimatyzacji. Przez bezpieczeństwo rozumie się stan, w którym jednostka lub grupa społeczna czy organizacja nie odczuwają zagrożenia swojego istnienia lub podstawowych interesów.

Z punktu widzenia BI najważniejsze jest bezpieczeństwo życia i zdrowia ludzi, następnie bezpieczeństwo zgromadzonego mienia oraz bezpieczeństwo technologiczne. Nad utrzymaniem bezpieczeństwa czuwają: system sygnalizacji pożarowej, system oddymiania, system automatycznego gaszenia pożaru, dźwiękowy system ostrzegawczy, system wykrywania gazów trujących, system sygnalizacji włamania i napadu, system kontroli dostępu, system telewizji dozorowej, system sterowania windami, system ochrony zewnętrznej budynku, system kontroli dostępu do parkingów oraz system monitorowania procesów technologicznych[13].

3.1 ZARZĄDZANIE BEZPIECZEŃSTWEM

Zarządzanie bezpieczeństwem budynków BI dotyczy działań profesjonalnych, tzn. opartych na rzetelnej wiedzy, fachowych umiejętnościach, racjonalnych metodach, sprawnych oraz skutecznych sposobach i technikach postępowania. Istotą jest zarządzanie rozumiane jako dążenie do osiągania celów poprzez planowanie, organizowanie, motywowanie i kontrolowanie ludzi i oddanych im do dyspozycji zasobów. W obecnych, bardzo skomplikowanych czasach najlepszym rozwiązaniem jest wprowadzenie globalnego systemu zarządzania bezpieczeństwem BI, czyli stworzenie tzw. polityki bezpieczeństwa BI. Polityka ta będzie przemyślanym zbiorem reguł i praw oraz sposobów postępowania w przypadkach pojawienia się zagrożeń. Musi mieć niestety charakter przymusowy i dotyczyć całości działalności w budynku.

W BI typu biurowego, a tych jest zdecydowana większość, główne zagrożenia bezpieczeństwa pochodzą od własnych pracowników, kontrahentów, kooperantów i zwykłych intruzów.

Oceniając bezpieczeństwo, należy zwrócić szczególną uwagę na wyraźnie wyodrębnione trzy fazy funkcjonowania BI[14]:

– faza nocna (zamknięcie lub stan czuwania),
– faza pośrednia (sprzątanie przed lub po godzinach pracy, przygotowanie do użytkowania),
– faza dzienna (pełne użytkowanie).

Fazy funkcjonowania obiektu wpływają na zmiany profilu występujących zagrożeń oraz na zakres i charakter wybranego zagrożenia. Dlatego zapewnienie bezpieczeństwa BI w każdej z faz wymaga odrębnej analizy ryzyka i oceny możliwości wystąpienia potencjalnych zagrożeń. Analiza powiązań pomiędzy zagrożeniami, parametrami obiektu i zastosowanymi zabezpieczeniami wymaga traktowania budynku BI jako obiektu o systemowej analizie bezpieczeństwa. Bezpieczeństwo BI opracowuje się i wdraża, stosując odpowiednie algorytmy projektowania systemów ochrony, które obejmują kategorie chronionych obiektów, poszukują słabych miejsc, w których mogą wystąpić zagrożenia, określają środki neutralizacji zagrożeń i dokonują czasowej analizy skuteczności ochrony. Czasowa analiza skuteczności jest najważniejsza, ponieważ określa, czy czas potrzebny na fizyczną interwencję i ujęcie sprawcy jest mniejszy od czasu zmaterializowania się zagrożenia.

Aby ułatwić organizację i rozmieszczenie systemów zabezpieczeń, wprowadza się w chronionym obiekcie tzw. strefy bezpieczeństwa. W najbardziej ogólnej analizie wyróżnia się trzy podstawowe strefy bezpieczeństwa: peryferyjną, obwodową i wewnętrzną. Ich rozległość i odległość od najbardziej chronionego pomieszczenia czy przedmiotu zależy od konkretnego rodzaju obiektu. Najdalej od chronionego miejsca znajduje się strefa peryferyjna, którą jest przeważnie bezpośrednie otoczenie obiektu. Strefa obwodowa oddziela strefę peryferyjną od strefy wewnętrznej. Tworzą ją (przeważnie) mury budynku wraz z otworami okiennymi i drzwiami. Strefa

bezpośrednio przyległa do chronionego pomieszczenia to tzw. strefa wewnętrzna z głównym chronionym dobrem.

3.2 STRUKTURY ZARZĄDZANIA A BEZPIECZEŃSTWO POŻAROWE

Stosowana obecnie struktura zarządzania bezpieczeństwem budynku za pomocą systemów: SMS *(Security Management System),* DMS *(Danger Management System)* lub też tradycyjnie jeszcze BMS *(Building Management System)* to przede wszystkim systemy techniczne, których działanie oparto na technologiach informatycznych. Wyróżnić można dwie główne grupy tych systemów:

– systemy zabezpieczające ludzi i mienie przed skutkami zagrożeń losowych,

– systemy zabezpieczające ludzi i mienie przed skutkami zagrożeń wynikających ze świadomej działalności człowieka[15].

Największym zagrożeniem losowym dla budynku jest zawsze pożar, dlatego też do grupy pierwszej należą głównie systemy pożarowe: SSP, system automatycznego gaszenia, system oddymiania i dźwiękowy system ostrzegawczy DSO. Inne zagrożenia losowe to burze, wichury, powodzie, trzęsienia ziemi.

Podstawowym zadaniem systemu SSP jest szybkie wykrycie pożaru w jego początkowym stadium, zanim ogień osiągnie rozmiary trudne do opanowania. W razie wykrycia i potwierdzenia zagrożenia centrala SSP podejmuje decyzję o zainicjowaniu alarmu pożarowego odpowiedniego stopnia oraz koordynuje działania praktycznie wszystkich elementów ochrony przeciwpożarowej w danym obiekcie.

Systemy automatycznego gaszenia mają za zadanie rozpoczęcie gaszenia ognia, by stłumić pożar w początkowej fazie i zapobiec jego rozprzestrzenieniu się. W zależności od rodzaju i przeznaczenia pomieszczeń są wyposażone w różne środki gaśnicze Powstający w czasie pożaru dym rozprzestrzenia się w krótkim czasie, powodując dezorientację ludzi. Składniki chemiczne dymu stanowią groźbę utraty przytomności bądź nawet uduszenia. Rola systemu oddymiania polega na usuwaniu dymu oraz ciepła ze strefy pożaru, co umożliwia przeprowadzenie sprawnej ewakuacji. Do sprawnego przeprowadzenia ewakuacji ludzi z zagrożonej strefy służy system DSO. System ten powiadamia ludzi o niebezpieczeństwie i kieruje ich na odpowiednie ciągi ewakuacyjne. Obecnie stosuje się systemy z informacją głosową, gdyż ostrzeganie w postaci syren wywoływało przeważnie panikę lub było lekceważone. Ponadto informacja głosowa jest zrozumiała dla wszystkich użytkowników obiektu.

Do drugiej grupy systemów należą: system sygnalizacji włamania i napadu (SSWiN), system kontroli dostępu (SKD), system telewizji dozorowej (STVD). W grupie tej znajdują się również zagrożenia atakami terrorystycznymi. System SSWN pełni dwojaką rolę w obiekcie: sygnalizuje wystąpienie napadu – funkcja aktywna w czasie normalnej pracy oraz sygnalizuje wystąpienie włamania – funkcja aktywna w czasie, gdy obiekt jest zamknięty. W przypadku automatycznego wykrycia włamania

lub próby włamania do chronionego obiektu system sygnalizuje alarm w sposób dźwiękowy lub świetlny oraz przesyła informację do centrum monitorowania. W razie napadu istnieje możliwość ręcznego uruchomienia systemu. W przypadku napadu, ze względu na nieprzewidzianą reakcję napastnika, alarm nie powinien być sygnalizowany ani akustycznie, ani dźwiękowo. Podstawowe zadanie systemu SKD polega na monitorowaniu oraz porządkowaniu przemieszczania się ludzi, jak również pojazdów, w dozorowanych strefach. W ten sposób system zabezpiecza obiekt przed dostępem osób niepowołanych oraz ogranicza poruszanie się osób nieuprawnionych po wydzielonych strefach, pozostawiając jednocześnie swobodę przemieszczania osobom uprawnionym.

System STVD umożliwia ciągłą i kompleksową obserwację wielu obszarów chronionego obiektu z jednego lub kilku stanowisk monitorowania oraz archiwizację zapisu wizji. System ten wspomaga pozostałe systemy odpowiedzialne

za bezpieczeństwo obiektu poprzez umożliwienie bieżącej weryfikacji zaistniałych zdarzeń oraz możliwość odtworzenia zdarzeń z materiałów archiwalnych, tworząc w ten sposób materiał dowodowy[16].

Każdy z systemów zabezpieczeń ma podobną strukturę funkcjonalną. Głównym elementem jest centrala albo sterownik, do którego podłączone są różnego rodzaju czujki. Dobór czujek zależy od przewidywanego sposobu materializacji zagrożeń. Z centralą lub sterownikiem musi być zapewniona komunikacja za pomocą urządzeń wejściowych, centrala musi mieć także możliwość przesyłania poprzez urządzenia wyjściowe sygnału alarmu do określonego miejsca lub centrum monitorowania. Centrale współpracują z innymi systemami w ramach integracji.Bardzo istotnym zagadnieniem jest metoda integracji systemów. Ze względu na pewność i niezawodność działania integracja profesjonalnych systemów zabezpieczeń jest przeważnie dokonywana na poziomie oprogramowania w programach integrujących na stacjach operatorskich. Jest to jednak najwolniejszy sposób integrowania systemów z powodu długich czasów przetwarzania informacji, szczególnie w dużych rozbudowanych systemach. Wyjątkowo w obiektach, które nie podlegają obowiązkowi ochrony systemami sygnalizacji pożaru, np. w małych biurach czy domach jednorodzinnych, popularne są zintegrowane centrale obejmujące np. ochronę pożarową budynku i zabezpieczenie przed napadem i włamaniem. Jest to sposób integracji wykonany na bazie sprzętu.

BI kryje w swych wnętrzach systemy automatycznego sterowania używane do zarządzania bezpieczeństwem, komfortem i komunikacją. Współczesne systemy sterowania budowane są na bazie urządzeń i sieci komputerowych. Należy zawsze pamiętać, że podstawowym zagrożeniem dla systemów zarządzających inteligentnym budynkiem jest nieautoryzowane wtargnięcie do systemu poprzez sieć komputerową. Dlatego sieć ta wymaga szczególnie starannego zarządzania bezpieczeństwem, zwłaszcza z coraz powszechniejszym otwieraniem się sieci komputerowych na dostęp do Internetu. Z powodu coraz szerszego zastosowania sieci Ethernet z protokołem TCP/IP do komunikacji pomiędzy urządzeniami poszczególnych systemów poprzez sieć obiektową sieć ta powinna podlegać takim samym procedurom zarządzania

ruchem i bezpieczeństwem jak sieć komputerowa. Znaczenie zarządzania bezpieczeństwem sieci obiektowej często jest niedoceniane, co może spowodować, iż pewnego dnia jakiś zmęczony haker włamie się do systemu zarządzania IB zamiast do innego komputera. Resztę scenariusza dopisać można sobie samemu.

PODSUMOWANIE

Mimo że trudno przewidzieć jakie rozwiązania techniczne przyniesie przyszłość, wiadomo, że założenia inteligentnego budynku się nie zmienią lub ulegną kosmetycznym modyfikacjom. Oczywiste jest, że bez względu na rewolucje technologiczne, zawsze będzie się dążyło do zmniejszenia poboru energii elektrycznej, wzrostu wydajności klimatyzacji, uproszczenia i redukcji okablowania, zwiększenia mobilności użytkujących budynek ludzi, a także ich bezpieczeństwa i zdrowia.

Powstaną programy wspomagające proces projektowania. Będą zapewniały analizy i podpowiedzi dla projektantów, zapewnia łatwą interpretację danych i wygenerują wszystkie niezbędne dokumenty projektowe. Pozwolą na modelowanie zachowań budynku i stworzą bazę danych dostępną dla uczestników procesu projektowania, dzięki czemu będzie możliwość łatwego osiągnięcia zakładanych parametrów budynku. Programy te wspomogą również utrzymanie, konserwacje i ewentualną modernizację budynku. Stworzone zostaną również narzędzia diagnostyczne pozwalające na automatyczne uruchamianie systemów budynkowych , automatyczną diagnostykę i ciągłą optymalizacje nastaw. Powstaną udoskonalone algorytmy adaptacyjne i samonastawne, bazujące na sieciach neuronowych. Zaistnieją możliwości zakupu z najtańszych źródeł poprzez sieć i zostanie podniesione bezpieczeństwo transakcji. Opracowane zostaną zaawansowane techniki wizualizacji i analizy danych pozwalające w łatwy i skuteczny sposób wyszukiwać obszary do poprawienia. Rozpowszechnią się narzędzia do bezpiecznego monitorowania systemów budynkowych przez internet. Wspólne bazy danych będą zawierały dane archiwalne i bieżące z systemów wentylacji i klimatyzacji, oświetlenia i bezpieczeństwa. Rozwiną się jednorodne standardy danych pozwalające na ich łatwą wymianę pomiędzy poszczególnymi podsystemami, standaryzacji ulegną również sposoby symulacji zachowań budynków, uruchomienia i regulacji.

osługując się analogią do historii inteligentnego budynku można przewidzieć, że będzie kontynuowane dążenie do miniaturyzacji urządzeń i jeszcze większej integracji różnych podsystemów. Po upływie pewnego czasu być może zniknie pojęcie inteligentnego budynku, ponieważ wszystkie obiekty będą spełniać stawiane dziś wymagania, a pojawi się idea „budynku myślącego”.

BIBLIOGRAFIA

[1] Chmielewski J., Rykowski J., *Automatyczna generacja zintegrowanego interfejsu „człowiek-maszyna” na potrzeby inteligentnego budynku*, materiały Katedry Technologii Informacyjnych, Uniwersytet Ekonomiczny, Poznań 2009

[2] http://www.hotelarze.pl/prawo-turystyka/zalecenie-poz-1986.php . Zalecenie Rady 86/666/EWG z dnia z dnia 22 grudnia 1986 r.
[3] DG ELPRO Ludwinów - inteligentny budynek u stóp Wawelu, mat.www.interia.pl
[4] Masły D., Kierunki rozwojowe oceny jakości środowiska zbudowanego na przykładzie wybranych metod badań jakościowych w architekturze. Koncepcja oceny jakości budynków biurowych w warunkach polskich, praca doktorska, Politechnika Śląska, Gliwice 2004
[5] Mikulik J., Budynek inteligentny, tom II: Podstawowe systemy bezpieczeństwa w budynkach inteligentnych, Wydawnictwo Politechniki Śląskiej, Gliwice 2005
[6] Masły D., Jakość budynków biurowych w świetle najnowszych metod oceny jakości środowiska zbudowanego, Wydawnictwo Politechniki Śląskiej, Gliwice 2009
[7] Mikulik J., Budynek inteligentny, tom II: Podstawowe systemy bezpieczeństwa w budynkach inteligentnych, Wydawnictwo Politechniki Śląskiej, Gliwice 2005.
[8] Wong J. K. W., Li H., Wang S. W., Intelligent Building Research: A Review, Automation in Construction, Number 14, Elsevier 2005
[9] Wigginton M., Harris J., Intelligent Skins, Architectural Press, Oxford UK, 2002
[10] Chun To Cho M., Fellows R. Intelligent Building Systems in Hong Kong Offices, Facilities, Volume 18, Number 5-6, MCB University Press, 2000
[11] Przewidywane trendy rozwoju poszczególnych standardów automatyki budynkowej do roku 2028 (źródło:Conference Dual Sourcing Vs. Sole Sourcing for Building Automation Controls, Washington, November 2005)
[12] Clements-Croome D. – 2nd International Congress on Intelligent Building Systems, Cracow 2002
[13] Niezabitowska E. – Budynek inteligentny, Politechnika Śląska, Gliwice 2005,
[14] Ehrlich P.P. – What is an intelligent building, AutomatedBuilding. com, August 2005,
[15] Mikulik J. – Budynek inteligentny, tom II: Podstawowe systemy bezpieczeństwa w budynkach inteligentnych, Wydawnictwo Politechniki Śląskiej, Gliwice 2005,
[16] Blim M, Mikulik J. – Security management of office facilitiesin the situation of contemporary threats, proc. of 4th International Congress on Intelligent Building Systems, InBuS2006, AGH Cracow, 2006,

Článok recenzoval:
Ing. J. Svetlík, PhD.