Instalacje inteligentnego budynku

Krzysztof Duszczyk, Andrzej Dubrawski, Albert Dubrawski, Marcin Pawlik, Mariusz Szafrański

Zadaniem współczesnych instalacji budynkowych jest zapewnienie odpowiedniego komfortu życia i pracy, bezpieczeństwa ludzi i mienia przy jednoczesnym obniżeniu kosztów eksploatacji. Realizacja tych zadań wymaga wykorzystania wielu elementów pomiarowych, sterujących oraz wykonawczych, działających zgodnie z opracowanymi algorytmami. Inteligentne instalacje budynkowe należy traktować jako zbiór innowacyjnych technologii, dzięki którym można zapewnić efektywne i przyjazne środowisko, pozwalające na realizację założonych, wielowątkowych celów.

1. Instalacje HVAC

Instalacje HVAC (*Heating, Ventilation, Air Conditioning*) – ogrzewania, wentylacji i klimatyzacji – należą do najbardziej energochłonnych instalacji budynkowych. Jednym z celów stosowania inteligentnej automatyki w instalacjach HVAC jest więc obniżenie kosztów zużycia energii. Obecnie nowoczesne systemy HVAC działają na podstawie analizy warunków środowiska zewnętrznego i wewnętrznego, monitorowana jest również obecność osób w pomieszczeniach. Stosowane są programy czasowe, pozwalające zmniejszyć moc ogrzewania oraz wyłączyć wentylację i nawilżanie powietrza w okresie nieobecności pracowników (w nocy, w dni wolne od pracy, urlopy), co wpływa na mniejszy pobór energii elektrycznej przez pompy, wymienniki ciepła i inne urządzenia wchodzące w skład tego systemu.

Dla powietrza wewnętrznego określa się również inne parametry, do których należą:

- prędkość cyrkulacji powietrza – nie powinna przekraczać 0,2 m/s;
- proporcja tlen/dwutlenek węgla – zbyt niska zawartość tlenu powoduje niedotlenienie, a zbyt wysokie stężenie dwutlenku węgla w powietrzu stanowi zagrożenie dla układu oddechowego;
- zawartość substancji organicznych – trujące substancje organiczne nawet w niewielkim stężeniu mogą powodować negatywne reakcje organizmu (zmęczenie, senność i dekoncentrację);
- zawartość cząstek stałych – cząstki te (kurz, dym papierosowy) wpływają negatywnie na układ oddechowy;
- zawartość alergenów – te elementy (roztocza, zarodniki grzybów, zarodniki pleśni, pyłki roślin) mogą być niebezpieczne nie tylko dla alergików,
- zawartość mikroorganizmów –organizmy te (wirusy, glony, bakterie) stanowią zagrożenie dla zdrowia ludzkiego.

Ogrzewanie, wentylacja i klimatyzacja służą do wytworzenia odpowiedniego mikroklimatu w pomieszczeniu, czyli nadania ww. parametrów. Instalacje tych trzech systemów muszą ze sobą ściśle współpracować. Do zapewnienia odpowiednich parametrów powietrza w pomieszczeniu służą takie urządzenia, jak: klimatyzatory, osuszacze i nawilżacze, oczyszczacze (filtry i biofiltry), wentylatory, grzejniki, jonizatory. W dużych obiektach budowlanych są instalowane centrale wentylacyjno-klimatyzacyjne.

Centrale wentylacyjno-klimatyzacyjne są kompleksowymi systemami służącymi do kształtowania środowiska naturalnego w budynku. Jedną z klasyfikacji central jest ich podział z uwagi na realizowane funkcje. Są to centrale: wywiewne, nawiewne oraz nawiewno-wywiewne.

Centrale wywiewne

Najprostsze – służą do usuwania powietrza z pomieszczeń. Sterowanie ich pracą polega głównie na regulacji natężenia przepływu powietrza wywiewanego. Zazwyczaj składają się z przepustnicy wielopłaszczyznowej, wentylatora oraz jednego lub dwóch filtrów powietrza.

Centrale nawiewne

Służą do dostarczania odpowiedniej ilości powietrza o określonych parametrach (uzdatniania powietrza zewnętrznego). Składają się (oprócz wentylatora i filtrów) z nagrzewnic, chłodnicy oraz nawilżacza powietrza.

Centrale nawiewno-wywiewne

Najbardziej skomplikowane – realizują funkcje wyżej wymienionych central, zapewniając jednocześnie dużą sprawność. Jest to możliwe dzięki wykorzystaniu urządzeń służących do odzysku ciepła (lub chłodu) z powietrza wywiewanego i przeniesienia do powietrza nawiewanego. Wykorzystywane są wymienniki: krzyżowe, rotacyjne, z czynnikiem pośredniczącym, pompy ciepła oraz wymienniki typu rurka ciepła. Wysoka wydajność takich wymienników ciepła pozwala na znaczną redukcję kosztów eksploatacji systemów klimatyzacyjnych. Jednoczesne wykorzystywanie kilku technologii, np. odzysk dwustopniowy (pompa ciepła i recyrkulacja) lub trzystopniowy (pompa ciepła, wymiennik krzyżowy i recyrkulacja), pozwala na odzyskiwanie nawet do 95% energii.

Podstawowym parametrem centrali klimatyzacyjno-wentylacyjnej jest natężenie przepływu powietrza. Wartość tego parametru jest zależna od rodzaju budynku, jego wielkości i przeznaczenia. Wyznaczana jest na podstawie określonych norm. Centrale o średnich i dużych wydajnościach mogą być budowane jako sekcyjne (blokowe, modułowe) lub kompaktowe. Centrale o małych wydajnościach to zazwyczaj rozwiązania kompaktowe.

Wyposażenie central stanowią elementy automatyki, takie jak: czujniki (temperatury, wilgotności, ciśnienia, zawartości

różnych składników powietrza), presostaty, termostaty, zawory, siłowniki itp. Podstawowym elementem każdej centrali są wentylatory montowane w sekcji nawiewnej i wywiewnej, napędzane silnikami elektrycznymi sterowanymi za pomocą przekształtników częstotliwości (falowników). Zastosowanie falowników umożliwia płynną regulację wydatku wentylatorów, zapewniając jednocześnie wysoką sprawność regulacji.

W celu zagwarantowania odpowiedniej jakości powietrza stosowane są różnego rodzaju filtry. Ich zadaniem jest usuwanie z powietrza zanieczyszczeń, takich jak pyły, bakterie czy wirusy. Stosowane są filtry różnych klas: na wlocie powietrza do centrali filtry wstępne (klasa G), na wylocie filtry dokładne (klasa F) lub absolutne (klasa H).

Odpowiednią temperaturę powietrza zapewniają nagrzewnice i chłodnice. Wykorzystywane są nagrzewnice wodne (glikolowe) lub elektryczne, a także gazowe lub olejowe. Najpopularniejszym rozwiązaniem są nagrzewnice wodne. W systemie chłodzenia wykorzystywane są chłodnice wodne lub freonowe. Chłód dostarczają wytwornice wody lodowej (chillery lub agregaty absorpcyjne). Chłodnice są wykorzystywane również do osuszania powietrza.

Dla zapewnienia odpowiedniej wilgotności powietrza stosuje się nawilżacze kanałowe, komory zraszania lub wytwornice elektryczne i gazowe.

Oprócz wypełniania standardowych funkcji dotyczących kształtowania środowiska naturalnego w budynku centrala wentylacyjno-klimatyzacyjna musi realizować określone scenariusze bezpieczeństwa. Opracowuje się dla niej tzw. matrycę sterowań, która opisuje zachowanie się centrali w przypadku wystąpienia aktywnego alarmu (np. pożarowego) lub awarii istotnych urządzeń.

2. Instalacja oświetleniowa

Nowoczesna instalacja oświetleniowa musi spełniać szereg wymagań. Dotyczą one zarówno estetyki wykonania opraw oświetleniowych i włączników, zastosowania energooszczędnych źródeł światła, konieczności zapewnienia wymaganego natężenia oświetlenia, jak i współpracy z innymi systemami inteligentnego budynku. W celu zapewnienia wymaganego poziomu natężenia oświetlenia instalacja powinna być wyposażona w odpowiednie regulatory oraz współpracować z układem sterowania żaluzji. Jej zadaniem jest zapewnienie właściwego komfortu pracy lub mieszkania przy jednoczesnym zmniejszeniu zużycia energii elektrycznej. W celu realizacji tych działań stosuje się sterowanie natężeniem oświetlenia, uwzględniające pory dnia (dzień, noc), a także aktualne nasłonecznienie. Oświetlenie jest załączone tylko wtedy, gdy w pomieszczeniu znajduje się użytkownik (sterowanie wspomagane przez informację z czujników ruchu i czujników zmierzchowych). Możliwe jest również tworzenie scen świetlnych, czyli aranżacja oświetleniowa według indywidualnych upodobań.

Nowoczesna instalacja oświetleniowa to instalacja z obwodami sterowania oddzielonymi od obwodów sieciowych. Można ją wykonać jako instalację niezależną od pełnego okablowania albo jako instalację oświetlenia całego obiektu, w ścisłym powiązaniu z multimedialnym okablowaniem strukturalnym. Dzięki rozdzieleniu obwodów sterowania i obwodów sieciowych w obwodach wyłączników występuje niskie napięcie. Można więc korzystać w pełni z multimedialnego okablowania strukturalnego.

W pierwszym okresie rozwoju systemów inteligentnego budynku producenci oferowali własne opracowania i rozwiązania w zakresie sterowania oświetleniem. Obecnie znakomita większość producentów obok własnych rozwiązań umożliwia (przez odpowiednie interfejsy) wykorzystanie dedykowanego dla sterowania oświetleniem systemu DALI *(Digital Addressable Lightning Interface*). Producenci oferują sterowniki DALI do różnych sieci obiektowych (BACnet, KNX, LCN, Modbus itp.), co przy dostępnym szerokim spektrum modułów I/O pozwala na tworzenie rozwiązań umożliwiających realizację nawet bardzo złożonych zadań (również ograniczających pobór energii). DALI jest właściwie standardem komunikacyjnym między elementami końcowymi sieci (czyli interfejsami opraw oświetleniowych) a systemem sterującym. Protokół sterowania w standardzie DALI (w połączeniu z kontrolerami i sensorami) działa w topologii Master-Slave. Oświetleniowa magistrala cyfrowa jest dwuprzewodowa, składa się z centralnego sterownika sterującego jedną lub kilkoma liniami. Do jednej linii DALI można przyłączyć do 64 indywidualnie adresowanych urządzeń z wbudowanymi modułami DALI (stateczniki do świetlówek, regulatory natężenia oświetlenia, styczniki, przekaźniki), które mogą zostać przyporządkowane do każdej z 16 zdefiniowanych grup. Umożliwia to indywidualne wysterowanie każdej oprawy, realizację scen świetlnych oraz sygnalizację uszkodzenia źródła lub modułu. W porównaniu do klasycznego systemu sterowania oświetleniem występuje dwukierunkowy przepływ informacji między systemem sterującym a oprawami. Działanie systemu DALI nie polega jedynie na realizacji poleceń użytkownika (operatora), lecz także na zbieraniu i analizie informacji dostarczanych przez czujniki umieszczone przy urządzeniach końcowych. Obecnie system DALI należy oceniać jako rozwiązanie nowoczesne, spełniające oczekiwania użytkowników. Analizując jednak aktualną sytuację na rynku oraz trendy w rozwoju automatyki budynkowej (np. upowszechnianie się komunikacji bezprzewodowej), można się spodziewać, że technologia bazująca na zwykłych przewodach miedzianych (którą jest system DALI) zostanie w pewnym momencie zastąpiona przez nowsze rozwiązania. Zastosowanie systemu DALI wymaga układania dedykowanych kabli w ścianach i sufitach, co sprawia, że rozwiązanie to jest technicznie i ekonomicznie zasadne wyłącznie w przypadku budowy nowych obiektów lub znacznej modernizacji już istniejących.

3. Systemy bezpieczeństwa (SMS, DMS)

W obecnych czasach (z uwagi na powszechne zagrożenie terroryzmem) systemy bezpieczeństwa stanowią nieodzowny element wyposażenia praktycznie każdego nowo budowanego obiektu. Dotyczy to budowli o rozmaitej kubaturze i przeznaczeniu. W zależności od funkcji danego obiektu i jego wielkości zastosowanie niektórych systemów bezpieczeństwa jest obligatoryjne, unormowane prawnie. Można wyróżnić następujące systemy bezpieczeństwa:

- System Kontroli Dostępu (SKD);
- System Sygnalizacji Włamania i Napadu (SSWiN);

- System Telewizji Dozorowej (CCTV – *closed-circuit television*);
- Dźwiękowy System Ostrzegawczy (DSO);
- System Sygnalizacji Pożarowej (SSP).

Często w literaturze systemy te określa się akronimem SMS (*Security Management Systems*) lub DMS (*Danger Management Systems*).

Zapewnienie odpowiedniego poziomu bezpieczeństwa obiektu (bezpieczeństwa ludzi i mienia) stanowi jedno z ważniejszych zadań dla każdego projektanta, właściciela czy użytkownika budynku. W zależności od obiektu rola poszczególnych systemów jest zróżnicowana. Konieczność ich stosowania, jak i ich funkcje stanowią wypadkową wynikającą z obowiązujących przepisów, analizy zagrożeń oraz wymagań użytkownika. Systemy te mogą działać autonomicznie lub pracować w sposób zintegrowany. Dynamika rozwoju systemów bezpieczeństwa jest bardzo duża. Szczególną uwagę zwraca się na ich integrację, co w konsekwencji pozwala na osiągnięcie bardzo wysokiego poziomu bezpieczeństwa.

3.1. System Kontroli Dostępu (SKD)

Ten system zabezpiecza obiekt przed dostępem osób nieuprawnionych. Elementy Systemu Kontroli Dostępu stanowią:

- sterownik (kontroler) dostępu;
- karty identyfikacyjne (breloki);
- czytnik nośnika indentyfikacyjnego;
- mechaniczne urządzenia blokujące;
- oprogramowanie.

Sterownik dostępu to urządzenie mikroprocesorowe odpowiedzialne za wszelkie zdarzenia w systemie związane z wejściem do określonej strefy i wyjściem z niej. Sterownik obsługuje czytniki kart i urządzenia blokujące przejście. Odczytuje informacje zawarte na karcie identyfikacyjnej i weryfikuje ich prawdziwość, następnie – zgodnie z programem zapisanym w jednostce centralnej – blokuje sterowane przejście lub nie blokuje go. Jako karty identyfikacyjne mogą być wykorzystywane:

- karty z kodem kreskowym;
- karty magnetyczne;
- karty z kodem odczytywanym na podczerwień;
- karty pojemnościowe;
- karty typu Wiegand;
- karty elektroniczne (chipowe) pamięciowe i procesorowe;
- karty zbliżeniowe.

Karty z kodem kreskowym

Należą do najprostszych rozwiązań. Kod kreskowy jest nanoszony indywidualnie na każdą kartę w procesie personalizacji. Niemożliwa jest zmiana czy też usunięcie raz zapisanej informacji. Są jednak łatwe do skopiowania. Ten niski stopień bezpieczeństwa spowodował odejście od wykorzystywania tych kart w SKD.

Karty magnetyczne

Wyróżnia się dwa rodzaje kart magnetycznych: karty Lo-Co (*Low Coercivity*) i karty Hi-Co (*High Coercivity*). Na kartę naniesione są trzy ścieżki z materiału magnetycznego. Dane są zapisywane w formie bitów. Każdy ze znaków, których na ścieżce może być 40, jest kodowany kombinacją 5 bitów. Karty Lo-Co charakteryzują się niskim współczynnikiem koercji paska magnetycznego, są więc podatne na niebezpieczeństwo rozmagnesowania i utraty zapisu. Ich zaletą jest niska cena. Te właściwości sprawiają, że karty Lo-Co są wykorzystane w masowych, mniej odpowiedzialnych zastosowaniach, np. w systemach parkingowych. Karty Hi-Co wykonane są z materiałów o znacznie wyższych parametrach, co powoduje, że są bardziej odporne na rozmagnesowanie i utratę zapisu, są więc dużo bezpieczniejsze.

Karty Wieganda

Są standardem przemysłowym. Wykorzystują zjawisko generacji impulsów w specjalnym drucie o małej średnicy i specyficznych właściwościach magnetycznych (rdzeń drutu jest wykonany z materiału magnetycznie miękkiego, a zewnętrzne warstwy z materiału magnetycznie twardego). Drut wtopiony w kartę jest poddawany działaniu zewnętrznego zmiennego pola magnetycznego. Podczas zmiany natężenia pola w drucie powstaje impuls Wieganda, odbierany i interpretowany przez czytnik. Ilość danych zapisanych na karcie nie przekracza 40 bitów. Raz zapisanej informacji nie można zmienić. Karty takiej również nie można podrobić. Karty mogą być wykorzystywane w dużym przedziale temperatur (od –80 do +260°C). Karty Wieganda w SKD stosuje się głównie do pomieszczeń o zwiększonym stopniu różnego typu zagrożeń (silne pola elektromagnetyczne, duża rozpiętość temperatur, zagrożenie chemiczne).

Karty elektroniczne (chipowe) pamięciowe i procesorowe

Zawierają pamięć elektroniczną (karty pamięciowe) lub specjalny mikroprocesor (karty procesorowe). Umożliwiają wielokrotny zapis i odczyt informacji. Zapewniają duże bezpieczeństwo zapisu. Dla kart pamięciowych możliwy jest zapis (do 32 kB danych) tylko do wybranych obszarów pamięci.

Karty procesorowe oferują jeszcze większe bezpieczeństwo zapisu, umożliwiając dokonywanie operacji związanych z autoryzacją (np. porównanie hasła dostępu). Objętość zapisywanych danych wynosi od 1 do 16 kB. Karty chipowe mogą być dodatkowo chronione czterocyfrowym kodem PIN. Karty elektroniczne umożliwiają odczyt danych z odległości 5 do 15 cm.

Karty zbliżeniowe

Występują dwa podstawowe typy kart zbliżeniowych: pasywne i aktywne. Źródłem zasilania dla kart pasywnych jest pole elektromagnetyczne wytwarzane przez czytnik (energia pobierana jest przez kartę w momencie zbliżenia jej do czytnika). Karty aktywne mają zasilanie bateryjne, a pole czytnika stanowi jedynie informację aktywującą. Karty zbliżeniowe do odczytu informacji nie potrzebują bezpośredniego kontaktu z czytnikiem. Karty wyposażone są w płaskie anteny radiowe, które powodują, że orientacja przestrzenna karty przy kontakcie z czytnikiem nie ma dużego znaczenia.

Karty zbliżeniowe współpracują z czytnikami, które mają za zadanie przyjąć informację zawartą na karcie, zweryfikować ją i przesłać do sterownika dostępu. Często spotykane są czytniki z podwójną weryfikacją użytkownika (karta + kod PIN).

Z uwagi na swoje zalety karty zbliżeniowe są najchętniej i najczęściej wykorzystywanymi kartami w SKD.

Mechaniczne urządzenia blokujące skutecznie ograniczają dostęp do pomieszczeń, stref, budynków osobom do tego nieuprawnionym. Należą do nich: bramki, śluzy, kołowroty, elektrozaczepy, elektrozwory.

Elektrozaczepy

Istnieją dwa rodzaje elektrozaczepów: standardowe i rewersyjne. Elektrozaczepy standardowe są odblokowywane w momencie podania napięcia na zaciski zasilające. W zaczepie rewersyjnym podanie napięcia powoduje jego blokowanie. W sytuacjach alarmowych, np. w przypadku pożaru, urządzenia blokujące powinny dawać się automatycznie bądź ręcznie odblokować. Z uwagi na ten wymóg w SKD stosuje się elektrozaczepy rewersyjne.

Elektrozwory

Pełnią podobną funkcję jak elektrozaczepy. Składają się z dwóch części – modułu zawierającego cewkę elektromagnesu i zwory magnetycznej przykręcanej do skrzydła drzwi. Elektrozwory nie mają żadnych części ruchomych i dzięki temu pracują bezgłośnie. Ich działanie jest podobne do działania elektrozaczepu rewersyjnego.

Oprogramowanie SKD

Dedykowane oprogramowanie narzędziowe pozwala na utworzenie systemu, który steruje pracą czytników, zarządza uprawnieniami dostępu, jak również monitoruje i archiwizuje pracę całego SKD. Oprogramowanie umożliwia tworzenie obszernych baz danych osób wraz z bazą wszystkich kart, kodów PIN, uprawnień dostępu do określonych stref, pomieszczeń itp.

Rejestracja i przechowywanie baz danych zwiększa bezpieczeństwo systemu np. w przypadku uszkodzenia czytnika lub utraty jego pamięci (istnieje możliwość ponownego wgrania danych do pamięci czytnika). Operator może wprowadzać do systemu nowe osoby, nadając każdej z nich uprawnienia z podziałem na strefy dostępu, strefy czasowe i datę ważności. Może również blokować kartę (np. w przypadku jej utraty) lub zmieniać uprawnienia dostępu do poszczególnych stref. Istnieje możliwość tworzenia ekranów wizualizacyjnych, ułatwiających kontrolę poprawności działania systemu. Na stacjach roboczych, na podstawie map bitowych, zobrazowane są wszystkie elementy systemu, co umożliwia łatwą ocenę stanu pracy poszczególnych urządzeń. Wykorzystywana jest również funkcja tworzenia i wydruku raportów.

Używanie w SKD nawet najbardziej skomplikowanych haseł dostępu czy niedających się podrobić kart nie pozwala na jednoznaczną identyfikację osoby. Cel ten można zrealizować, wykorzystując biometrię. Identyfikacja biometryczna jest bardzo dynamicznie rozwijającą się dziedziną. Polega na identyfikacji osób na podstawie informacji biologicznych (cech fizycznych – mierzonych w danej chwili) lub behawioralnych (nabytych – zmiennych w czasie). Takimi cechami są np. odciski palców, wielkość i geometria dłoni, geometria twarzy, a także budowa anatomiczna oka czy głos. Biometria jest stosowana w systemach kontroli dostępu już od lat siedemdziesiątych ubiegłego wieku. Do najpopularniejszych technologii biometrycznych wykorzystywanych w SKD można zaliczyć technologie:

- linii papilarnych;
- rozpoznawania geometrii dłoni;
- cech oka (tęczówka, siatkówka);
- rozpoznawania geometrii twarzy;
- analizy głosu.

Technologia linii papilarnych

Najpopularniejszy sposób biometrycznej identyfikacji i weryfikacji osób. Wykorzystywane są dwie metody: optyczna i pojemnościowa. W optycznej używany jest zwykły skaner optyczny z odpowiednim oprogramowaniem. Obraz opuszki palca (po przyłożeniu do skanera) jest utrwalany w postaci obrazu cyfrowego, a następnie porównywany z wcześniej zapisanym wzorcem. Czas operacji (rejestracja i weryfikacja danych) nie przekracza 1 s. Wadą metody optycznej jest dość duża wrażliwość na zabrudzenia, tłuszcze, wodę czy głębsze uszkodzenia powierzchni skóry, co może powodować błędne odczyty.

W metodzie pojemnościowej wykorzystywany jest specjalny czujnik pojemnościowy, który mierzy różnicę pojemności i głębokości bruzd w głębi skóry. Czytniki linii papilarnych korzystające z tej metody są znacznie skuteczniejsze w przypadku identyfikacji osób o pokaleczonych, zabrudzonych czy mokrych palcach.

Do zalet tych metod biometrycznej identyfikacji można zaliczyć relatywnie niską cenę urządzeń i obróbki danych, natomiast do wad uprzedzenia z uwagi na wykorzystanie ich w kryminalistyce.

Systemy oparte na rozpoznawaniu geometrii dłoni

W systemach tych wykorzystywany jest trójwymiarowy obraz tworzony przez oświetlenie dłoni promieniami podczerwonymi i odczytanie obrazu matrycą CCD. Po umieszczeniu dłoni na specjalnym czytniku zostają wykonane trójwymiarowe zdjęcia dłoni oraz pomiary różnych cech charakterystycznych dłoni (ok. 90 pomiarów). Wzorzec wraz z przypisanym do niego numerem ID przechowywany jest w pamięci (bazie danych) systemu. Proces autoryzacji polega na przyłożeniu dłoni do czytnika i wpisaniu na jego klawiaturze numeru ID. Bieżący obraz porównywany jest ze wzorcem w bazie danych. Wpisanie numeru ID przyspiesza proces weryfikacji, który trwa ok. 1 s. Wskaźniki błędnych odczytów są na poziomie ok. 0,1%.

Systemy oparte na rozpoznaniu cech oka

Systemy te są bardzo skuteczne. Oferowany poziom bezpieczeństwa należy do najwyższych ze wszystkich istniejących i dostępnych na rynku metod biometrycznych.

Metoda analizy siatkówki oka

Polega na skierowaniu strumienia światła podczerwonego (o małym natężeniu) przez źrenicę na dno oka. Kamera cyfrowa o wysokiej rozdzielczości odbiera obraz odbity od siatkówki, a system komputerowy tworzy wzorzec danych referencyjnych

siatkówki. Wzorzec ten jest zapisywany w bazie danych, a następnie wykorzystywany przy każdej weryfikacji i identyfikacji. Czas trwania weryfikacji i identyfikacji wynosi ok. 2 s. Wskaźniki błędnych odczytów są na poziomie ok. 0,00005%. Z uwagi na fakt, że odczyt wymaga przystawienia oka do urządzenia pomiarowego, metoda ta jest uważana za inwazyjną.

Metoda analizy tęczówki

W metodzie tej nie ma konieczności przystawienia oka do urządzenia pomiarowego. Kamera sama odnajduje twarz, oko i tęczówkę. Kamera cyfrowa o wysokiej rozdzielczości rejestruje obraz tęczówki. Na podstawie tego obrazu system komputerowy tworzy unikalny cyfrowy kod zawierający skrócony opis charakterystycznych cech tęczówki. Istnieje aż 266 punktów charakterystycznych tęczówki. Często dla zapewnienia jeszcze większego bezpieczeństwa kod ten jest szyfrowany. Przechowuje się go w bazie danych i używa przy każdej weryfikacji. Do podjęcia decyzji, czy oko, które obserwuje kamera, żyje, dokonywana jest analiza ruchu gałki ocznej bądź analiza dynamiki zmian średnicy źrenicy. Czas trwania weryfikacji i identyfikacji wynosi średnio ok. 2 s. Producenci zaawansowanych czytników tęczówki oka podają poziom błędów rzędu 10^{-10} lub nawet 10^{-20}.

System rozpoznawania twarzy

Identyfikacja jest realizowana na podstawie cech geometrycznych twarzy. Zależności pomiędzy poszczególnymi częściami twarzy z wiekiem nie ulegają znaczącym zmianom. Ludzka twarz ma wiele cech biometrycznych: cechy geometryczne (kształt brwi, kształt nosa, kształt ust, kształt podbródka), cechy antropometryczne (odległość między środkami oczu, odległości pomiędzy oczami i nosem, odległość między linią oczu a linią ust). Na podstawie zarejestrowanego obrazu tworzona jest geometryczna siatka charakterystycznych punktów twarzy, która stanowi matematyczny wzorzec danej osoby zapisywany w bazie. Po obróbce i matematycznym przekształceniu obrazu twarzy jest on porównywany ze wzorcem wcześniej zarejestrowanym. Najczęściej jest zapamiętywanych kilka wzorców rysów twarzy, a pomiar jest dokonywany za pomocą kilku kamer, aby uzyskać obraz przestrzenny. Porównywanie nigdy nie jest dokonywane między obrazami, lecz między punktami charakterystycznymi rysów twarzy.

Metoda rozpoznawania rysów twarzy jest łatwa w użyciu, nieinwazyjna i akceptowalna przez użytkowników. Współczesne algorytmy rozpoznawania, opierające porównanie na analizie punktów charakterystycznych twarzy, powodują, że odczyt jest niezależny od używania szkieł kontaktowych, okularów, zmian fryzury, zarostu itp. Skuteczność systemu jest bardzo wysoka, bliska 100%.

System oparty na analizie głosu

Każdy człowiek ma indywidualne cechy głosu, takie jak tempo, dynamika, częstotliwość czy chwilowe widmo mowy. Na podstawie analizy tych parametrów komputer buduje i zapisuje w bazie danych wzorzec w postaci cyfrowej. Identyfikacja użytkownika polega na porównaniu wczytanego wzorca z głosem osoby mówiącej hasło do mikrofonu. Z uwagi na to, że głos rozpoznawany na podstawie jednej znanej frazy, może zostać podrobiony (np. z wykorzystaniem wysokiej klasy aparatury audio), stosuje się rozpoznawanie na podstawie kilku zmieniających się fraz.

Bezpieczniejszy sposób rozpoznawania głosu opiera się na identyfikowaniu mówiącego na podstawie analizy brzmienia jego głosu. Najnowsze metody analizy głosu przetwarzają na bieżąco dowolną wypowiedź mówiącego i pozwalają na ciągłe sprawdzanie tożsamości osoby w trakcie trwania rozmowy. W niektórych rozwiązaniach metoda ta jest łączona z weryfikacją posiadanej wiedzy. Nowoczesne rozwiązania zawierają specjalistyczne oprogramowania, z wbudowanymi algorytmami pozwalającymi na ograniczenie wpływu szumów środowiskowych i wahań głosu użytkownika na poprawność działania systemu. Metoda analizy głosu jest łatwa w użyciu, społecznie akceptowalna i tania, jednak nie daje takiej skuteczności i niezawodności jak systemy biometryczne omówione wcześniej. Z uwagi na wielkie możliwości w jej stosowaniu prowadzone są intensywne prace nad jej ulepszaniem.

Systemy Kontroli Dostępu poza funkcją bezpieczeństwa mogą w obiekcie realizować dodatkowe funkcje, takie jak kontrola czasu pracy czy kontrola przebywania w określonych strefach.

3.2. System sygnalizacji włamania i napadu (SSWiN)

Zadaniem systemów SSWiN jest reagowanie na próby naruszenia chronionej strefy, a w przypadku dokonania włamania wykrycie intruza. Istnieją dwie odmienne koncepcje realizacji tych układów. Według jednej koncepcji w przypadku stwierdzenia naruszenia strefy chronionej generowany jest jedynie sygnał alarmowy powiadamiający odpowiednie służby ochrony o zaistniałej sytuacji. Układ śledzi intruza, który nie zdaje sobie sprawy z faktu, że został odkryty. Pozwala to na ujęcie sprawcy na gorącym uczynku. Według drugiej koncepcji należy potencjalnego intruza odstraszyć. W przypadku stwierdzenia naruszenia strefy chronionej załączane są syreny oraz oświetlenie alarmowe. Określa się cztery kategorie zagrożeń: od Z1 (niska kategoria zagrożenia) do Z4 (najwyższa kategoria zagrożenia). Do poszczególnych kategorii zagrożeń przypisane są klasy systemów alarmowych (SA1 do SA4). Określa się również klasy urządzeń alarmowych:

- A – popularna;
- B – standardowa;
- C – profesjonalna;
- D – specjalna.

Urządzenia alarmowe są przyporządkowane do klas systemów: SA1 → A, AS2 → B, SA3 → C, SA4 → D. W skład systemu SSWiN wchodzą: centrala, czujki, przyciski antynapadowe, sygnalizatory akustyczno-optyczne.

Centrala alarmowa

Stanowi podstawowy element systemu. Jest wyposażona w wejścia i wyjścia alarmowe, pamięć zdarzeń, układ kontroli stanu zasilania oraz złącze magistrali rozszerzeń. Dodatkowo ma wejścia i wyjścia swobodnie programowalne. Do zadań centrali alarmowej należą:

- zbieranie i analiza sygnałów pochodzących od poszczególnych czujek;

- rejestracja i archiwizacja sygnałów i zdarzeń;
- aktywacja i dezaktywacja alarmów;
- sterowanie wybranymi urządzeniami wykonawczymi.

Do najczęściej wykorzystywanych czujek w SSWiN można zaliczyć: kontaktrony, bariery podczerwieni, czujki ruchu, czujki zbicia szkła, detektory gazu.

Kontaktrony

Są wykorzystywane do zabezpieczania okien, drzwi i bram. Kontaktron to para styków wykonanych z materiału ferromagnetycznego, zamkniętych w szklanej bańce, oraz zewnętrzny magnes trwały. Styki pod wpływem zewnętrznego pola magnetycznego się przyciągają. W wyniku oddalenia magnesu tracą połączenie, tworząc przerwę w obwodzie. Montaż kontaktronu polega na umieszczeniu magnesu na ruchomej części zabezpieczanego obiektu (skrzydło drzwi lub okna), a części ze stykami na nieruchomej części. Konstrukcyjnie kontaktrony dzielą się na kontaktrony do montażu wpuszczanego lub powierzchniowego.

Bariery podczerwieni

Mają szerokie zastosowanie w ochronie samego obiektu (bariery w wykonaniu wewnętrznym), jak i terenu (bariery w wykonaniu zewnętrznym). Bariery w wykonaniu wewnętrznym są wykorzystywane do zabezpieczania okien, drzwi i przejść, natomiast bariery w wykonaniu zewnętrznym stosuje się do ochrony obwodowej. Bariery emitują wiązki promieniowania podczerwonego. Modele wewnętrzne mają zasięg dochodzący do 750 m, modele zewnętrzne – do 500 m. Są wyposażane w automatykę dostosowującą czułość bariery do zmiennych warunków atmosferycznych.

Czujki ruchu

To najczęściej stosowane detektory w systemach SSWiN. Czujki dzielą się na czujki PIR i czujki dualne. Działanie czujki PIR polega na detekcji promieniowania podczerwonego. Każdy obiekt, którego temperatura jest wyższa od 0°K emituje promieniowanie podczerwone. Element piroelektryczny zainstalowany w czujce rejestruje zmiany promieniowania. System mikroprocesorowy przetwarza dane i decyduje, czy zmiany promieniowania w monitorowanym obszarze są na tyle duże, żeby aktywować alarm. Zastosowanie prostych czujek PIR nie zawsze jest skuteczne. Czujniki tego typu mogą w niektórych sytuacjach generować fałszywe alarmy. W celu ograniczenia ich liczby stosuje się czujki dualne – oprócz piroelementu mają one tor mikrofalowy. Wykrycie zaburzenia jedynie w torze podczerwieni nie generuje alarmu, inicjuje go dopiero zaburzenie występujące równocześnie w torze podczerwieni i mikrofalowym. Czujki ruchu występują w wersjach szerokokątnych i o zwiększonym zasięgu. Kąt detekcji czujek może być regulowany (np. przez zaklejenie części okienka). Oprócz czujek przeznaczonych do montażu na ścianie istnieją czujki montowane na suficie. Obszar detekcji takich czujek jest okręgiem. Istnieje możliwość regulacji promienia okręgu i wykluczania pewnych obszarów w postaci wycinków koła. Czujki sufitowe występują zarówno w wersji PIR, jak i dualnej.

Czujki stłuczeniowe

Są czujkami mikrofonowymi. W wyniku zastosowania wielostopniowych selektywnych wzmacniaczy są szczególnie czułe na sygnały o wysokich częstotliwościach (pękanie szkła), nie reagują natomiast na inne hałasy zewnętrzne. Czujki te reagują także na sygnały o niskiej częstotliwości (uderzenia podczas tłuczenia). Materiały pochłaniające dźwięk (np. zasłony) zmniejszają zasięg ich działania.

Czujki wstrząsowe

Reagują na drgania mechaniczne podłoża, do którego są przymocowane. Najczęściej montowane są na drzwiach, oknach, ścianach i stropach chronionego pomieszczenia. Czujki wstrząsowe umożliwiają przebywanie użytkownika w pomieszczeniu przy załączonym systemie alarmowym, tworząc tzw. ochronę obwodową.

Detektory gazu

Rolą detektorów gazu jest wczesne wykrycie i powiadomienie o przekroczeniu krytycznego stanu określonego gazu. Poza zapewnieniem bezpieczeństwa zdrowiu i życiu (czujki toksycznego tlenku węgla – czadu czy gazu ziemnego z kuchenki gazowej) detektory gazu mogą pełnić istotną funkcję w ochronie przed włamaniem. Stosowany przez włamywaczy gaz usypiający może być szybko wykryty przez czujkę gazu usypiającego – chloroformu.

Przycisk antynapadowy

Naciśnięcie go wywołuje natychmiastowy alarm. Przycisk powinien być ukryty w dyskretnym miejscu, aby użytkownik obiektu w momencie zagrożenia mógł go użyć w sposób niezauważony, oraz zabezpieczony przed przypadkowym naciśnięciem.

Sygnalizatory

Mogą być akustyczne lub akustyczno-optyczne. Oprócz emisji dźwięku o natężeniu powyżej 75 dB emitują również sygnały świetlne. Sygnalizatory SSWiN w zależności od środowiska pracy występują jako wewnętrzne lub zewnętrzne.

3.3. System telewizji dozorowej CCTV

System telewizji dozorowej stanowi zestaw elementów i urządzeń wykorzystywanych do wizyjnego dozorowania określonych stref obiektu lub terenu. Podstawowymi elementami systemów CCTV są:

- urządzenia do obserwacji wizyjnej: kamery, monitory i ekrany wizyjne;
- urządzenia do przetwarzania i rejestracji obrazu: multipleksery, krosownice, pamięci;
- urządzenia transmisyjne: nadajniki, odbiorniki i modemy;
- oprogramowanie zarządzające.

Kamery występujące w systemach CCTV można podzielić ze względu na rozmaite kryteria:

- tryb pracy (monochromatyczne, kolorowe, dualne);
- sposób montażu (stałopozycyjne – kompaktowe i kopułkowe, obrotowe – zintegrowane i nie);
- rodzaj sygnału wyjściowego (analogowe – wyjście BNC, IP – wyjście sieciowe LAN).

Kamery monochromatyczne

Reagują na promieniowanie z zakresu widzialnego (400–770 nm), a także na promieniowanie z zakresu bliskiej podczerwieni (770–850 nm). Dzięki temu można je stosować do obserwacji nocnych z wykorzystaniem reflektorów podczerwieni emitujących światło niewidoczne dla ludzkiego oka.

Kamery kolorowe

Z uwagi na konieczność przekazywania informacji o kolorze mają mniejszą rozdzielczość niż kamery monochromatyczne. Dodatkowo cechują się mniejszą czułością. Jednak ze względu na możliwość przekazywania obrazu w kolorze są powszechnie stosowane.

Kamery dualne

Wykorzystują zalety obu wyżej wymienionych typów kamer. Jedno urządzenie jest jednocześnie kamerą kolorową i monochromatyczną. Cel ten osiągnięto przez zastosowanie ruchomego filtru podczerwieni. W trybie kolorowym filtr jest umieszczony przed przetwornikiem. Przy zmniejszeniu jasności światła docierającego przez obiektyw do środka kamery zostaje odsunięty filtr i kamera przechodzi w tryb pracy monochromatycznej. Poniżej zostaną wymienione kamery stałopozycyjne.

Kamery kopułkowe

Są to zintegrowane jednostki wyposażone w obiektyw i elektronikę sterującą. Stosuje się w nich obiektywy o stałej lub zmiennej ogniskowej w zakresie 2–12 mm, czyli od ultraszerokokątnych do teleobiektywów.

Kamery kompaktowe

W odróżnieniu od kamer kopułkowych nie są jednostkami zintegrowanymi. Kamery kompaktowe stosuje się tam, gdzie mają działać odstraszająco i gdzie nie jest wymagane ich ukrycie. Mogą być montowane w pomieszczeniach i na zewnątrz budynku. Zarówno kamery kopułkowe, jak i kompaktowe mogą być monochromatyczne, kolorowe lub dualne.

Kamery obrotowe

Są wyposażone w dwie ruchome osie (pochylanie i obracanie) napędzane przez silniki. Nowoczesne kamery umożliwiają obserwację prędko poruszających się obiektów z szybkością obrotową do 400°/s. Kamery są wyposażone w pierścienie ślizgowe, aby nie ograniczać kąta obrotu. Mogą mieć funkcje cyfrowej stabilizacji obrazu, śledzenia poruszających się obiektów czy tworzenia tzw. stref prywatności. Kamery szybkoobrotowe mogą być wyposażone w interfejsy sieciowe LAN.

Kamery z wyjściem analogowym i kamery IP

W instalacjach CCTV spotyka się obecnie dwa rodzaje kamer: analogowe i IP. Kamery analogowe są wyposażone w wyjścia wizyjne typu BNC. Systemy te są stopniowo wypierane przez nowoczesne rozwiązania, oparte na technologii sieci komputerowych (systemy IP). W systemach IP dane wizyjne są transmitowane przez sieć komputerową. Strumień danych może zostać odebrany w dowolnym miejscu sieci przez urządzenia rejestrujące obraz lub konwertujące go na sygnał analogowy w celu wyświetlenia. Strumień wizyjny może być jednocześnie zapisywany i wyświetlany na komputerze podłączonym do sieci.

Rejestracja obrazu

Pierwsze aplikacje CCTV były wyposażane w magnetowidy. Obecnie ich rolę przejęły rejestratory cyfrowe. Obraz może być rejestrowany z prędkością do 25 kl/s, co zapewnia płynność obrazu, lecz wymaga znacznej przestrzeni dyskowej. Rozmiary dysków zainstalowanych w rejestratorach osiągają znaczne rozmiary: od 80 GB do kilku TB. Jeśli pamięci dyskowe są niewystarczające, stosuje się zewnętrzne macierze dyskowe. Oprócz macierzy podłączanych bezpośrednio do urządzeń rejestrujących używane są macierze, do których dostęp jest realizowany za pośrednictwem sieci komputerowej LAN. Aby ograniczyć obszar zajętości pamięci, a jednocześnie zachować pełnię możliwości systemu SSWiN, rejestracja obrazu prowadzona jest z wykorzystaniem dodatkowych funkcji. Wykorzystuje się np. detekcję ruchu. Obraz jest rejestrowany z małą poklatkowością (1 kl/s), dopiero w przypadku wykrycia ruchu tryb zapisu zostanie przełączony i ma większą wartość, np. 12,5 kl/s.

Podobną rolę jak przy detekcji ruchu pełnią wejścia alarmowe. W przypadku wysterowania wejścia alarmowego rejestratora z którejś czujki systemu SSWiN tryb zapisu przełącza się, dając obraz o wyższej poklatkowości i jakości. Obecnie większość systemów ma funkcję detekcji ruchu informującą jedynie o zaistniałym zdarzeniu, bez jego specjalistycznej analizy. W praktyce nie każdy ruch wykryty przez czujnik jest zagrożeniem.

Współczesne systemy CCTV wykorzystują rozmaite techniki detekcji zdarzeń, pozwalające na analizę każdego zajścia i sugerujące sposób reakcji na analizowane zdarzenie. System samodzielnie może decydować o danym zdarzeniu i określać dokładność, z jaką dany obraz ma być rejestrowany. Obecnie jest tendencja do przeniesienia wszystkich procesów odpowiadających za detekcję ruchu z rejestratorów i dedykowanych urządzeń do nowoczesnych kamer przemysłowych IP. Te inteligentne kamery potrafią samodzielnie wykryć potencjalne zagrożenie i, współpracując z dedykowanym oprogramowaniem analizującym, kategoryzować je. Rozwój technik sieciowych umożliwia uproszczenie zarządzania systemem, pozwalając jednocześnie na równoległą rejestrację obrazu w różnych punktach sieci (bezpośrednio w pamięci kamery, na dysku lokalnego komputera czy dedykowanym rejestratorze). Zwiększa to bezpieczeństwo przechowywania danych. Również podgląd obrazu oraz dostęp do nagrań archiwalnych mogą być realizowane przez sieć komputerową.

Oprogramowanie zarządzające stanowi podstawę działania, monitorowania, analizy i zapisu. W wielu przypadkach wystarcza standardowa przeglądarka internetowa, dająca możliwości obserwacji za pomocą interfejsu wbudowanego w kamerę sieciową lub serwer wizyjny. Jest to zasadne wtedy, gdy jednocześnie wyświetlany jest obraz najwyżej z kilku kamer. Do jednoczesnej obsługi obrazów z wielu kamer konieczne jest dedykowane oprogramowanie zarządzające. Na rynku dostępna jest szeroka gama oprogramowań do zarządzania materiałem wizyjnym. Umożliwiają one:

- wyświetlanie na żywo, zapisywanie i odtwarzanie sekwencji obrazów;
- jednoczesne wyświetlanie i nagrywanie obrazów z wielu kamer;
- realizowanie kilku trybów nagrywania (ciągły, planowany, nagrywanie uruchamiane w razie alarmu);
- przetwarzanie obrazu z dużą liczbą klatek na sekundę oraz dużą ilością danych;
- wyszukiwanie nagranych zdarzeń;
- zdalny dostęp za pomocą przeglądarki internetowej;
- zarządzanie alarmami itp.

3.4. Dźwiękowy System Ostrzegawczy (DSO)

Obowiązek stosowania dźwiękowego systemu ostrzegawczego wynika z rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów. Określa ono rodzaje obiektów użyteczności publicznej, w których rozgłaszanie sygnałów ostrzegawczych i komunikatów głosowych dla potrzeb bezpieczeństwa osób w nich przebywających jest obligatoryjne.

System nagłośnieniowy służy do głosowego powiadomienia osób przebywających w obiekcie o ewentualnym wystąpieniu zagrożenia, takiego jak pożar, akt terrorystyczny czy inny stan, który może mieć wpływ na bezpieczeństwo ludzi. Nadawane komunikaty głosowe mają zapewnić sprawną, bezpieczną i skuteczną ewakuację osób przebywających w obiekcie. System DSO musi spełniać dużo wyższe wymagania odnośnie do parametrów akustycznych, samokontroli i redundancji, zasilania awaryjnego w porównaniu do tradycyjnych systemów nagłośnieniowych. Każdy instalowany system DSO musi mieć aktualne certyfikaty i świadectwa dopuszczenia wydane przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej (CNBOP). W systemach DSO po wykryciu zagrożenia komunikaty głosowe są nadawane automatycznie. Istnieje również możliwość ręcznego wywołania zaprogramowanego komunikatu. Każdemu z nich można nadać odpowiedni priorytet nadawania oraz poziom głośności. Aby zwiększyć niezawodność działania, system jest dodatkowo wyposażony w funkcję samokontrolowania. System monitoruje stan linii głośnikowych, zasilania głównego i rezerwowego, połączenia między głównym procesorem a wzmacniaczami. Awarie są natychmiast zgłaszane administratorowi systemu. Wszystkie alarmy gromadzone są w pamięci urządzenia zarządzającego komunikatami DSO. Dźwiękowe systemy ostrzegawcze są administrowane i monitorowane przez podłączenie do głównej jednostki sterującej DSO komputera z dedykowanym oprogramowaniem zarządzającym.

3.5. System sygnalizacji pożarowej (SSP)

Obowiązującym aktem prawnym w zakresie SSP jest wspomniane rozporządzenie Ministra Spraw Wewnętrznych i Administracji. Określono w nim obiekty, w których instalacja SSP jest obligatoryjna. Głównie są to duże budynki komercyjne i użyteczności publicznej, w których czasowo lub stale może przebywać określona liczba osób. Systemy sygnalizacji pożaru, zwane także systemami alarmu pożaru (SAP), służą do wczesnego wykrywania zagrożenia pożarowego, powiadamiania o tym zagrożeniu oraz wykonywania określonych funkcji sterujących, mających za zadanie ochronę życia ludzkiego i minimalizację strat materialnych. SSP są projektowane i instalowane zgodnie z indywidualnymi wymaganiami konkretnego obiektu, dlatego ich struktura, algorytm działania i zakres mogą być mocno zróżnicowane. W skład systemu SSP wchodzą:

- centrale sterowania systemem;
- czujki pożarowe (wysoko czułe sensory pożarowe reagujące na różne rodzaje zagrożenia, takie jak dym, ogień, temperatura);
- przyciski alarmowe;
- sygnalizatory dźwiękowe i świetlne.

Systemy sygnalizacji pożarowej muszą spełniać wszystkie normy oraz mieć aktualne atesty Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej (CNBOP). Podlegają komisyjnemu odbiorowi przez inspektorów z Państwowej Straży Pożarnej.

Centrala sterowania

Stanowi „serce" każdego SSP. Odbiera sygnały od czujek, analizuje dane i przekazuje sygnały do innych podzespołów. Jest urządzeniem integrującym wszystkie elementy systemu automatycznego wykrywania pożarów. Koordynuje pracę wszystkich urządzeń w systemie oraz podejmuje decyzję o zainicjowaniu alarmu pożarowego, wysterowaniu urządzeń sygnalizacyjnych i przeciwpożarowych oraz o przekazaniu informacji do systemu nadzoru lub centrum monitorowania. W zależności od ustawień parametrów centrali sterującej jest do dyspozycji czas (w skrajnym przypadku do 10 minut) na weryfikację alarmu przez upoważnione służby i podjęcie decyzji. W razie braku takiej decyzji automatycznie rozpoczyna się cały scenariusz zdarzeń. Alarm pożarowy może być również wywołany przez wciśnięcie ręcznego ostrzegacza pożarowego (ROP). W takim przypadku scenariusz pożarowy rozpoczyna się natychmiast, bez zwłoki.

Czujki pożarowe

Umożliwiają automatyczne identyfikowanie zarzewia pożaru. Mogą wykrywać dym (czujki punktowe i liniowe), ciepło (reakcja na szybki przyrost lub przekroczenie ustalonego progu temperatury) lub oba te czynniki (czujka dymu, ciepła, czujka dualna dymu i ciepła) albo ogień (reagują na promieniowanie podczerwone lub ultrafioletowe płomienia).

Czujka dymu

Reaguje na produkty spalania lub rozkładu termicznego. Ten rodzaj czujek dzieli się na jonizacyjne i optyczne.

Czujka ciepła

Jest detektorem wykorzystującym termistor o ujemnym współczynniku temperaturowym (typ NTC). Wykorzystany termistor ma bardzo małą masę, co powoduje szybkie reagowanie na zmiany temperaturowe.

Czujka płomienia

Wykrywa emitowane przez płomienie promieniowanie podczerwone lub ultrafioletowe.

Wielosensorowe czujki pożarowe

Są inteligentnymi detektorami, które przekształcają analogowe parametry pożarowe wbudowanych czujników na zapis cyfrowy i za pomocą numerycznych algorytmów podejmują decyzję o istnieniu zagrożenia.

Uzupełnieniem czujek są rozmieszczane na ciągach komunikacyjnych przyciski pożarowe (ręczne ostrzegacze pożarowe). System SSP może być zintegrowany z różnymi instalacjami technicznymi. Integracja daje nie tylko możliwości zaalarmowania o wykryciu pożaru, lecz także możliwość rozpoczęcia działań zmierzających do ograniczenia rozprzestrzeniania się ognia lub jego likwidacji. System może wykonać wiele czynności, takich jak: uruchomienie systemu tryskaczy, otwarcie klap dymowych, zainicjowanie wyłączenia niebezpiecznych urządzeń elektrycznych, gazowych, otwarcie drzwi ewakuacyjnych lub bramek kontroli dostępu.

4. Instalacja zasilająca inteligentnego budynku

Przerwy w dostawie energii elektrycznej mogą być przyczyną zdarzeń zagrażających zdrowiu i życiu ludzi oraz powodem poważnych strat finansowych ze względu na utratę danych, zakłócenia procesu technologicznego czy awarię urządzeń. Przerwy te mogą być spowodowane wieloma czynnikami, do których można zaliczyć:

- zjawiska atmosferyczne (wyładowania atmosferyczne, powodzie, ulewne deszcze, upały, wichury, pożary, trzęsienia ziemi);
- wady technologiczne i konstrukcyjne (awarie);
- bezmyślność obsługi;
- sabotaż;
- roboty ziemne.

Aby móc określać niezawodność zasilania, wprowadzone zostało pojęcie dostępności A (*availability*). Dostępność określa się zależnością:

$$A = MTBF / (MTBF + MTTR) \quad (1)$$

gdzie:

- MTBF – czas międzyawaryjnej pracy (*Mean Time Between Failure*);
- MTTR – czas naprawy (*Mean Time To Repair*).

Dopuszczalna suma przerw w zasilaniu zależy od tego, jak dużą niezawodność systemu gwarantowanego zasilania chcemy uzyskać. Dla przyjętych wartości A można wyznaczyć przerwy w zasilaniu. W skali roku wyniosą odpowiednio:

A = 99,9% – system może być pozbawiony zasilania przez ok. 9 godzin;
A = 99,9999999% – system może być pozbawiony zasilania przez ok. 30 ms.

Wybór określonej wartości A powinien stanowić rozsądny kompromis między spodziewaną niezawodnością zasilania a kosztami instalacji. Aby optymalnie zaprojektować instalację zasilającą, wprowadzono kategoryzację odbiorników energii elektrycznej pod względem wrażliwości na zanik zasilania. Odbiorniki podzielono na trzy kategorie.

Kategoria I

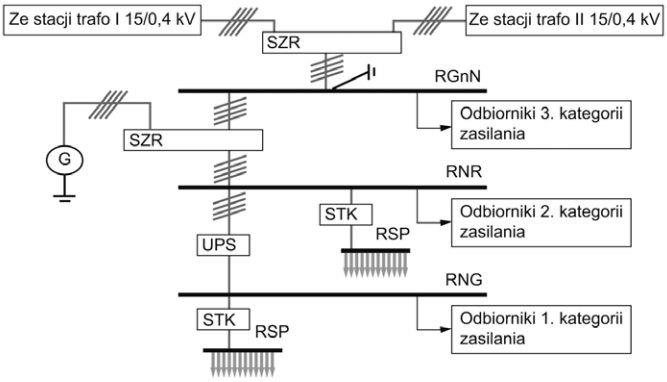
Odbiorniki strategiczne, nietolerujące nawet najmniejszych przerw w zasilaniu. Są to urządzenia wymagające zarówno ciągłości zasilania, jak i bardzo dobrych parametrów jakości energii elektrycznej. Należą do nich urządzenia telekomunikacyjne, informatyczne, medyczne.

Kategoria II

Odbiorniki, dla których kilkunastosekundowy zanik napięcia nie stanowi zagrożenia, a zasilanie musi być rezerwowane ze względu na ich znaczenie w systemie. Są to odbiorniki niewrażliwe na chwilowe zaniki napięcia czy zakłócenia impulsowe. Odporne są też na odchyły częstotliwości i wahania wartości skutecznej. Nie są podatne także na przepięcia. Należą do nich oświetlenie awaryjne, systemy wentylacji awaryjnej, urządzenia przeciwpożarowe.

Kategoria III

Odbiorniki bez znaczenia strategicznego dla budynku, niewymagające specjalnych warunków zasilania, np. oświetlenie ogólne, ogrzewanie, system wentylacji podstawowej. Schemat instalacji zasilającej inteligentnego budynku przedstawiono na rysunku 1.

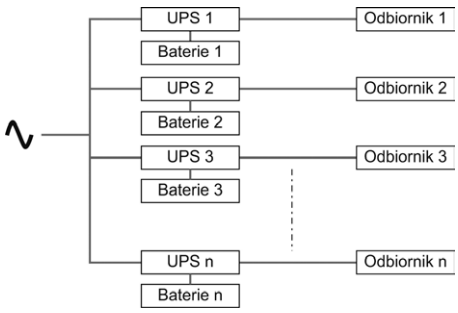


Rys. 1. Uproszczony schemat instalacji zasilającej inteligentnego budynku.
Legenda:
SZR – Samoczynne Załączenie Rezerwy;
STK – Siłownia Telekomunikacyjna;
UPS – zasilacz bezprzerwowy;
G – generator prądotwórczy;
RGnN – rozdzielnia główna niskiego napięcia;
RNR – Rozdzielnia Napięcia Rezerwowego;
RNG – Rozdzielnia Napięcia Gwarantowanego;
RSP – Rozdzielnia Stałoprądowa 48 V

Zgodnie z rysunkiem 1 zasilanie do RGnN może być dostarczane z dwu stacji transformatorowych, np. z I stacji transformatorowej 15/0,4 kV, a w momencie zaniku zasilania ze stacji I układ SZR przełącza pobór mocy na II stację transformatorową 15/0,4 kV. W chwili powrotu zasilania z pierwszej linii SZR powoduje ponowne zasilanie całego układu ze stacji I. Gdy wystąpi jednoczesny zanik zasilania z obu stacji transformatorowych, układ SZR wysyła sygnał uruchamiający

agregat prądotwórczy. W tym momencie rozdzielnia RGnN zasilająca odbiorniki III kategorii zostaje odłączona, a odbiorniki II kategorii tracą zasilanie, aż parametry napięcia zasilania dostarczanego przez agregat nie ustabilizują się na odpowiednim poziomie (kilkanaście do kilkudziesięciu sekund). Wtedy SZR przełącza RNR na zasilanie z agregatu i odbiorniki II kategorii odzyskują zasilanie. Odbiorniki podłączone do RSP i RNG, czyli odbiorniki I kategorii, są zasilane przez cały czas. Bezprzerwowe zasilanie zapewniają STK i UPS. W przypadku zaniku napięcia w sieci energetycznej energia do odbiorników I kategorii jest dostarczana z baterii akumulatorów. Zastosowanie układu UPS oraz agregatu prądotwórczego pozwala na znaczne ograniczenie pojemności baterii akumulatorów. Taka struktura uniezależnia działanie odbiorów kategorii I od zaburzeń występujących w zasilającej sieci energetycznej.

Jak już wspomniano, czas pracy baterii wynosi kilkanaście do kilkudziesięciu sekund potrzebnych do podjęcia pracy przez agregat prądotwórczy. Dzięki temu uzyskanie długiego czasu podtrzymania zasilania odbiorników pierwszej i drugiej kategorii zasilania nie wymaga rozbudowy systemu baterii. Czas podtrzymania zasilania awaryjnego może być dowolnie długi, jeśli tylko zapewni się odpowiedni system dostarczania paliwa do agregatu.



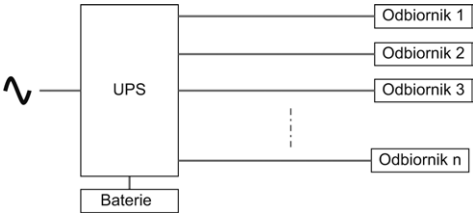
Rys. 2. Struktura rozproszona gwarantowanego zasilania

Całkowita moc agregatu prądotwórczego powinna bezpiecznie pokrywać zapotrzebowanie mocy przez odbiorniki I i II kategorii. Moc wyjściowa zasilacza UPS powinna być większa bądź równa sumie mocy wszystkich odbiorników kategorii I. Tak obliczoną moc wyjściową zasilacza UPS należy jeszcze dodatkowo powiększyć o ok. 10–20% na wypadek rozbudowy sieci odbiorów kategorii I. Prawidłowy dobór elementów systemu wymaga głębszej analizy, dotyczącej między innymi zainstalowanych urządzeń, ich mocy, prądów rozruchowych, zawartości harmonicznych itp. Można wyróżnić dwie podstawowe struktury układu gwarantowanego zasilania: rozproszoną i centralną. Struktura rozproszona, przedstawiona na rysunku 2, polega na zastosowaniu dedykowanych zasilaczy UPS dla każdego odbiornika. Do zalet systemu rozproszonego należą:

- niski koszt urządzeń;
- łatwość rozbudowy;
- możliwość wykorzystania istniejącej sieci zasilającej.

Do podstawowych wad systemu rozproszonego można zaliczyć:

- krótki czas podtrzymania pracy zasilanych urządzeń;
- małą trwałość baterii w zasilaczach;
- problemy z monitorowaniem i konserwacją.



Rys. 3. Struktura centralna gwarantowanego zasilania

Strukturę centralną przedstawiono na rysunku 3. W strukturze tej istnieje jeden główny zasilacz UPS oraz instalacja doprowadzająca gwarantowane napięcie do odbiorników.

Do zalet systemu centralnego rozproszonego należą:

- łatwość monitorowania i konserwacji zasilacza i baterii;
- długi czas podtrzymania przy pracy z baterii;
- możliwość zastosowania klimatyzacji pomieszczenia z zasilaczem i baterią, przedłużającej czas jej eksploatacji.

Do podstawowych wad systemu centralnego trzeba zaliczyć:

- wyższy koszt instalacji;
- konieczność wykonania instalacji gwarantowanego zasilania.

Możemy wyróżnić trzy podstawowe typy UPS-ów, będących głównym źródłem energii dla odbiorników I kategorii, pracujących w trybach offline lub online. Dla zasilaczy pracujących w trybie offline oraz *line-interactive* czas przełączania nie jest zerowy. W zasilaczach pracujących w trybie online prąd pobierany jest z baterii, która jest jednocześnie doładowywana z sieci energetycznej (lub – w przypadku jej awarii – z generatora). Dzięki takiemu rozwiązaniu przy awarii nie występuje przełączenie źródła zasilania odbiorników I kategorii, więc nie ma nawet najmniejszej przerwy w zasilaniu.

5. System monitoringu i zarządzania zużyciem mediów

System monitoringu i zarządzania zużyciem mediów to rozwiązanie, którego zadaniem jest monitoring online energii elektrycznej (z funkcją strażnika mocy zamówionej) oraz innych mediów (np. gazu, wody, ciepła). Systemy takie mogą być zrealizowane jako rozwiązania chmurowe. Zapewnia to użytkownikom możliwość monitoringu i zarządzania zużyciem mediów z dowolnego miejsca oraz eliminuje konieczność zakupu drogiego sprzętu (komputerów, serwerów). Na serwerze wirtualnym (w chmurze) pracuje aplikacja, która zbiera i analizuje online dane dotyczące zużycia wszystkich mediów. Dostęp do danych może odbywać się za pośrednictwem komputerów i urządzeń mobilnych (np. smartfonu, tabletu) z poziomu przeglądarki internetowej. Użytkownik ma stały dostęp zarówno do danych bieżących, jak i historycznych. ■

Fragment pochodzi z książki:
K. Duszczyk, A. Dubrawski, A. Dubrawski, M. Pawlik, M. Szafrański
Inteligentny budynek, Wydawnictwo Naukowe PWN, 2019