inwestor

Sąd Okręgowy
w Toruniu

Sąd Okręgowy w Toruniu
ul. Piekary 51
87-100 Toruń

Zakres opracowania	PROJEKT INSTALACJI TELETECHNICZNYCH INSTALACJE TELEINFORMATYCZNE INSTALACJE ELEKTRYCZNE	
Kategoria obiektu budowlanego	Kategoria XII	
Kody CPV	42961100-1 45311000-0	System kontroli dostępu Roboty w zakresie okablowania oraz instalacji elektrycznych

1. Spis treści

1. Spis treści 2
2. O p i s ogólny 5
   1. Przedmiot opracowania 5
   2. Podstawa opracowania 5
3. Wytyczne zabezpieczenia technicznego 7
   1. Interfejs użytkownika 7
      1. Tagi i identyfikacja 7
      2. Wymagania dotyczące rozpoznania tożsamości 7
      3. Czytniki kontroli dostępu powinny spełniać następujące wymagania 8
   2. Kontroler, interfejs przejścia kontrolowanego 8
   3. Konsola obsługi 9
      1. Wymagania w zakresie sygnalizacji i powiadamiania 9
      2. Program nadzorczy systemu kontroli dostępu powinien zapewniać 10
      3. Wymagania dotyczące zasilania 10
      4. Wymagania zabezpieczenia mechanicznego (kołowroty, bramki itp.) 10
      5. Dodatkowe funkcje systemu kontroli dostępu 10
      6. Integracja z systemem Rejestracji Czasu Pracy (RCP) 11
      7. Dane RCP 11
   4. Dodatkowe informacje 11
   5. Wymagania ogólne dotyczące systemu kontroli dostępu 12
   6. Architektura systemu 14
   7. Multiplikacja systemu 14
   8. Centralny System Zaręczania 14
   9. Drzwi wejściowe strefy kontrolowanej 15
   10. Czytniki kontroli dostępu 16
   11. Kontroler Przejścia 16
   12. Bramki kontroli dostępu 17
      1. Bramki dostępowe 17
      2. Obsługa niepełnosprawnych 17
      3. Integracja z SSP 17
   13. Specyfikacja techniczna elementów składowych systemu kontroli dostępu 18
      1. Serwer systemu 18
      2. Specyfikacja techniczna okablowania 18
      3. Przycisk wyjścia ewakuacyjnego 19
      4. Elektrozamek 19
      5. Zwora elektromagnetyczna z kontaktronem 20
      6. Karty zbliżeniowe 20
      7. Urządzenia dodatkowe 20

8. Zasilacze i obudowa 21
14. Zasilanie instalacji 21
15. Stanowisko ochrony 21
16. Stanowisko personalizacji kart 22
4. SYSTEM SYGNALIZACJI NAPADU I WŁAMANIA 22
1. Podstawy prawne opracowania, normy i wytyczne 22
2. Opis systemu 22
3. Wymagania dla systemu SSWiN 23
5. Okablowanie Strukturalne 23
1. Podstawa opracowania projektu 23
2. Wymagania ogólne dotyczące okablowania strukturalnego 24
3. Wymagania dla kabli symetrycznych 24
1. Wymagania dla ekranowanych kabli symetrycznych F/FTP kat.6A 24
6. SYSTEM REJESTRACJI C Z A S U PRACY (RCP) 27
1. Cel systemu rejestracji czasu pracy 27
2. Architektura systemu rejestracji czasu pracy 27
3. Wymagania ogólne dla systemu rejestracji czasu pracy 27
4. Funkcjonalność terminala systemu rejestracji czasu pracy 28
5. Terminal rejestracji czasu pracy 28
7. SYSTEM SYGNALIZACJI POZARU 30
1. Podstawa opracowania: 30
2. Podstawa opracowania: 30
3. Podstawa opracowania: 30
4. Charakterystyka obiektu 31
5. Wymagania dla systemu bezpieczeństwa 31
6. Opis ogólny systemu, lokalizacja urządzeń 32
1. Lokalizacja urządzeń systemu sygnalizacji pożarowej 32
7. Opis działania systemu 34
8. Opis urządzeń 34
1. Centrala Sygnalizacji Pożaru 34
2. Czujniki multisensorwe 36
3. Gniazda czujek 37
4. Wskaźnik zadziałania 37
5. Ręczny ostrzegacz pożarowy 37
6. Modułów Wejśc/Wyjść 37
7. Elementy systemu bezprzewodowego 38
9. Organizacja alarmowania 40
10. Montaż instalacji i prowadzenie okablowania 41
11. Zasilanie podstawowe i awaryjne 42
1. Centrala SSP zasilanie podstawowe 42
2. Centrala SSP Zasilanie awaryjne 42
8. M o n t a ż urządzeń i prowadzenie przewodów 43

1. Montaż bramek i systemu przyzywowego 43
2. Montaż kontrolerów i czytników 43
3. Prowadzenie instalacji. 44
1. Instalacja pozioma i pionowa 44
9. Bramki wykrywające metal 45
1. Bramka 45
2. Funkcje dodatkowe 45
3. Integracja 45
10. Kancelaria tajna 45
1. Wytyczne projektowania 45
11. Prowadzenie przewodów w trasach sugerowanych ..... **Błąd! Nie zdefiniowano zakładki.**
1. Kanał techniczny ciąg komunikacyjny budynku w Chełmnie ..... **Błąd! Nie zdefiniowano zakładki.**
1. Montarz rury kablowej w posadzce ..... **Błąd! Nie zdefiniowano zakładki.**
2. Prowadzenie tras na ścianach ..... **Błąd! Nie zdefiniowano zakładki.**
3. Materiały okładziny posadzki w korytarzu Partertu ..... **Błąd! Nie zdefiniowano zakładki.**

2. Opis ogólny

1. Przedmiot opracowania

Niniejszy projekt obejmuje wykonanie modernizacji Systemu Kontroli Dostępu (SKD) oraz powiązanych z nim Systemu Sygnalizacji Przeciwpożarowej (SSP) Systemu Sygnalizacji Włamania i Napadu (SSWiN) oraz systemu przyzywowego dla toalet publicznych.

2. Podstawa opracowania

Projekt niniejszy opracowano na podstawie:

- umowy na wykonanie dokumentacji projektowo - kosztorysowej,
- wytycznych inwestora,
- obowiązujących przepisów:
    - Rozporządzenie Ministra infrastruktury z dnia 12 kwietnia 2002r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie, Dz.U. Nr 75 poz. 690 z późniejszym zmianami,
    - Ustawa z dnia 20 grudnia 2021r. Prawo budowlane, Dz.U. 2021 poz. 2351
    - Ustawa z dnia 1 sierpnia 1998r. w sprawie oceny zgodności, wzoru deklaracji zgodności oraz sposobu znakowania wyrobów budowlanych dopuszczonych do obrotu i powszechnego stosowania w budownictwie, Dz.U. 1998 Nr 113 poz. 728
    - Dyrektywa Parlamentu Europejskiego I Rady 2014/34/UE w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do urządzeń i systemów ochronnych przeznaczonych do użytku w atmosferze potencjalnie wybuchowej
- i Polskich Norm:
    - PN-EN 60839-11-1:2014-01 - Systemy alarmowe i elektroniczne systemy zabezpieczeń -- cześć 11-1: Elektroniczne systemy kontroli dostępu -- Wymagania dotyczące systemów i komponentów
    - PN-HD 60364-1:2010 - instalacje elektryczne niskiego napięcia -- Część 1: Wymagania podstawowe, ustalanie og61nych charakterystyk, definicje
    - PN-HD 60364-4-41:2017-09 - instalacje elektryczne niskiego napięcia -- część 4-41: Ochrona dla zapewnienia bezpieczeństwa -- Ochrona przed porażeniem elektrycznym
    - PN-HD 60364-4-43:2012 - instalacje elektryczne niskiego napięcia -- część 4-43: Ochrona dla zapewnienia bezpieczeństwa -- Ochrona przed prądem przetężeniowym
    - PN-HD 60364-5-52:2011- instalacje elektryczne niskiego napięcia -- Część

5-52: Dob6r i Montaż wyposażenia elektrycznego - Oprzewodowanie

- PN-HD 60364-5-54:2011- instalacje elektryczne niskiego napięcia -- Część 5-54: Dob6r i Montaż wyposażenia elektrycznego -- Układy uziemiające i przewody ochronne
- SEP N SEP-E-002. instalacje elektryczne w obiektach budowlanych
- PN-EN 50173-1:2018-07 - Technika informatyczna -- Systemy okablowania strukturalnego -- część 1: Wymagania og61ne
- PN-EN 50174-1:2018-08- Technika informatyczna -- instalacja okablowania -- Część 1: Specyfikacja instalacji i zapewnienie jakości
- PN-EN 50174-2:2018-08 - Technika informatyczna -- instalacja okablowania -- część 2: Planowanie i wykonywanie instalacji wewnątrz budynków
- PN-EN 50174-3:2014-02 - Technika informatyczna -- instalacja okablowania -- Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków.

3. Wytyczne zabezpieczenia technicznego

Zastosowany system powinien być zgodny z zaleceniami normy PN-EN 60839-11-1 Systemy alarmowe i elektroniczne systemy zabezpieczeń, część 11-1: Elektroniczne systemy kontroli dostępu, wymagania dotyczące systemów i komponentów. System kontroli dostępu jako minimalne powinien spełniać wymagania stopnia 2. Zaleca się stosowanie systemu spełniającego wymagania stopnia 3.

System musi zawierać możliwość integracji z systemem rejestracji czasu pracy w postaci **automatycznego eksportu zdarzeń oraz spełniać wymagania Rozporządzenia Parlamentu** Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony os6b fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych - RODO, w zakresie anonimizacji danych osobowych (zalecana automatyczna anominizacja).

1. Interfejs użytkownika

1. Tagi i identyfikacja

Podstawowym nośnikiem tożsamości w SKD powinien być identyfikator w postaci T a g ` a wykonanej w technologii zapewniające szyfrowanie informacji oraz szyfrowana transmisje z czytnikiem (poprzez tag rozumiemy różne formy identyfikatorów wykorzystujących technologie RFiD).

W normalnym trybie działania system powinien wykorzystywany do rozpoznania pełną informacje identyfikatora w zależności od użytej technologii.

W awaryjnym trybie pracy system może wykorzystywany do rozpoznania jedynie część informacji identyfikatora (np. tylko kod obiektu), tryb awaryjny może zostać wymuszony brakiem komunikacji z serwerem SKD/RCP

Numer naniesiony dający s i ę odczytać z identyfikatora w postaci nadruku bądź przy użyciu programy lub skanera (np. mifare Tools) nie może być bezpośrednio reprezentacją pełnego kodowania.

W przypadku wykorzystania rozpoznania z a pomocą informacji zapamiętane w polaczeniu z identyfikatorem lub biometryka, informacja zapamiętana (kod PIN) wymaga minimum 4 cyfr. System powinien umożliwiać wykorzystanie czytników biometrycznych i w y k o r z y s t u j ą c y c h t e c h n o l o g i e M F A (m u l t i f a c t o r a u t h e n t i c a t i o n)

2. Wymagania dotyczące rozpoznania tożsamości

System powinien umożliwiać przyznawanie praw dostępu grupie danych identyfikacyjnych i oraz umożliwiać zmianę praw-dostępu grupy danych identyfikacyjnych. Tworzenie grup dostępowych, do których dopisane będą poszczególne indywidualne dane dostępowe, powinien też móc używać kodów QR i kodów EAN na potrzeby przyznawania praw (ścieżek dostępu) dla grupy goście z naniesionymi identyfikatorami na dokumentach)

3. Czytniki kontroli dostępu powinny spełniać następujące wymagania

- wykorzystywać protokół Wiegand-26 lub dłuższy do komunikacji, bądź podobny protokół producenta
- odporny na działanie czynników atmosferycznych, minimum IP55,
- częstotliwość pracy w zależności od wybranych tagów RFID
- kodowana transmisja danych pomiędzy czytnikiem i karta, klucz kodowania 64 bit,
- audiowizualna sygnalizację stanu drzwi (buzzer i/lub diody LED) bądź wyświetlacz TFT lub LCD
- zabezpieczenie przed odwrotna polaryzacja styków zasilających.
- styk antysabotażowy
- pracować jednocześnie na dwóch częstotliwościach 125KHz i 13,56 MHz
- odczytywać karty EM, HID oraz Mifare (ISO 14443A)
- sugerowany rozmiar czytnika powinien zawierac się w przedziale 35-80mm podstawy dolnej i 50x200mm wysokości

2. Kontroler, interfejs przejścia kontrolowanego

SKD powinien mieć wyjścia zdolne do sterowania elektromagnesów drzwiowych, zaczepów elektrycznych, aktywatorów montowanych w ościeżnicy, rygli sterowanych elektrycznie hydraulicznie albo pneumatycznie i/lub innych typów zamków elektromechanicznych oraz elektrycznych dźwigni przeciw panicznych, a także sterowania bezpotencjałowego bramkami uchylnymi, kołowrotkami. Kontroler powinien posiadać wejścia monitorujące stan drzwi (NC), oraz systemu SSP (przy czym rozłączenie elementów sterujących poprzez SSP realizowane będzie poprzez moduł I/O dedykowany na zasadzie rozłączenia zasilania.

- praca w trybie sieciowym (ON-LINE) i autonomicznym (OFF-LINE) samodzielna praca kontrolerów SKD tj. bez komunikacji z serwerem, w oparciu o posiadane dane konfiguracyjne w pełnym zakresie funkcjonalnym, buforowanie i rejestracja w pamięci nieulotnej zdarzeń do momentu odzyskania komunikacji z serwerem

- wielkość bufora, co najmniej 100 000 zdarzeń w każdym kontrolerze

- pojemność identyfikatorów użytkowników nie może być mniejsza, niż 26 000 osób.

- obsługa protokołu odczytu Wiegand 26/34/66 bitów

- możliwość rozszerzenia o dodatkowe 4 wejścia i 4 wyjścia

Praca w trybie autonomicznym każdego kontrolera powinna zapewniać zachowanie w pamięci nieulotnej uprawnień w zakresie dostępu dla użytkowników, oraz pozostałych parametrów związanych z działaniem kontrolowanego przejścia.

Każdy kontroler winien być wyposażony w dualną pamięć umożliwiającą wykonanie synchronizacji danych kontrolera z serwerem bez konieczności blokowania urządzań SKD (drzwi, kołowrotów, szlabanów) i użytkowników. Np. uprawnienie są zmienione w locie (komunikacja IP) nie ma to odczuwalnego wpływu na pracę urządzenie, tj mogą być wykonywane operacje równolegle (identyfikacja tagi, dodawanie uprawnień do tego samego kontrolera).

Jeden kontroler (sterownik) będzie obsługiwać maksymalnie jeden rodzaj przejścia.

Obudowa kontrolera (sterownika) powinna uniemożliwiać bezpośredni dostęp osobom nieuprawnionym.

Kontroler winien posiadać możliwość wyposażenia go w dodatkowe rozszerzenie alarmowe realizujące funkcję definiowanego alarmu manualnego, alarmu na obecność dymu bądź gazu w pomieszczeniu, alarmu sygnalizacji włamania oraz reakcji na alarm pożarowy. Płyta rozszerzeń musi posiadać co najmniej 4 wejścia oraz 4 wyjścia umożliwiające współpracę z innymi elementami jak czujniki otwarcia system ssp.

Dodatkowo kontroler (sterownik) powinien posiadać możliwość czasowego otwierania drzwi dowolną kartą celem zebrania numerów kart i ich autoryzacji.

Kontrolery mają zapewniać realizację funkcji „anti-passback", która uniemożliwia ponowne otwarcie danych drzwi w zadeklarowanym odstępie czasu, bądź bez uprzedniego przejścia do następnej strefy oraz funkcję "śluza", która uniemożliwi otwarcie danych drzwi przed fizycznym zamknięciem innych drzwi.

3. Konsola obsługi

1. Wymagania w zakresie sygnalizacji i powiadamiania

- sygnalizacja wizualna i/lub dźwiękowa stanu zaryglowania przejścia, aż do chwili przyznania dostępu,
- powiadamianie wizualne, gdy jest przyznany dostęp, rejestracja zdarzeń, gdy jest przyznany dostęp,
- powiadamianie wizualne, ostrzeganie i rejestracja zdarzeń, gdy odmowa dostępu nastąpiła w wyniku próby użycia przedawnionego identyfikatora,
- powiadamianie wizualne, ostrzeganie i rejestracja zdarzeń w przypadku odmowy dostępu w wyniku konfigurowalnej liczby prób użycia uprawnionego identyfikatora z nieuprawnioną informacją zapamiętaną,
- możliwość śledzenia karty (Wyświetlanie, rejestracja),
- możliwość śledzenia czytnika (Wyświetlanie, rejestracja).

Wszystkie zmiany inicjowane przez operatora powinny być rejestrowane z uwzględnieniem typu, ID operatora, czasu i daty wystąpienia,

2. Program nadzorczy systemu kontroli dostępu powinien zapewniać

- możliwość ograniczania praw dostępowych - okres ważności karty
- możliwość podglądu ruchu osobowego na wybranych przejściach w trybie on-line, dla wybranych typów zdarzeń (alarmowych) oraz przejść,
- współpracować ze skanerem dowodów osobistych i paszportów, dla kart gości,
- umożliwiać definiowanie kart dla gości, kart jednodniowych, kart okresowych,
- umożliwiać generowanie raportów ewakuacyjnych z uwzględnieniem ostatniej lokalizacji wszystkich pracowników i zarejestrowanych gości, obecnych na terenie budynku sadu,
- umożliwiać integrację z systemem depozytorów kluczy.

3. Wymagania dotyczące zasilania

Elementy systemu mogą być zasilane z linii NN 230VAC bądź za pomocą POE jednocześnie zapewniając podpięcie do sieci LAN (secure net)

4. Wymagania zabezpieczenia mechanicznego (kołowroty, bramki itp.)

- potwierdzenie pełnego obrotu w SKD,
- wspomaganie przejścia,
- blokada przed ruchem powrotnym,
- przycisk ewakuacyjny z sygnalizacją LED potwierdzającą użycie,
- użycie przycisku ewakuacyjnego odnotowane zostaje w SKD,
- drzwi objęte kontrola dostępu powinny być wyposażone w czujniki kontaktu potwierdzające otwarcie drzwi (np. kontaktrony).

5. Dodatkowe funkcje systemu kontrolidostępu

- możliwość dodawania kolejnych urządzeń w związku z rozbudową systemu,
- możliwość definiowania, dodawania oraz integracji z innymi urządzeniami związanych z automatyczna identyfikacją,
- możliwość integracji fragmentów systemu w sieciach LAN I WAN tj.
    - jednolite zarzadzanie elementami systemu rozmieszczonymi w różnych punktach,
    - możliwość obsługi dowolnej liczby obiektów.
- architektura oprogramowania typu Klient - Serwer,
- zabezpieczenie przed wczytywaniem niezaprogramowanych kart (np. kart płatniczych, urządzeń NFC).

- Monitorowanie zdarzeń alarmowych i napadowych oraz powiadamianie o nich

6. Integracja z systemem Rejestracji Czasu Pracy (RCP)

System RCP musi posiadać, możliwość współpracy z systemem ZSRK zamawiającego, za pośrednictwem, złącznika bazodanowego bądź pliku wymiany danych.

7. Dane RCP

Dane przekazywane między systemem RCP a HR ZSRK muszą być uzgodnione na poziomie wykonawstwa i integracji wybranego systemu RCP, system musi zapewnić wymianę danych oraz wprowadzać do użytku predefiniowane zdarzenia RCP jak wejście, wyjście, wyjście służbowe, wejście służbowe, przerwa, wyjście na żądanie itp. Schemat i oznaczenie kodowe należy uzgodnić z odpowiednim działem zamawiającego. Czytnik RCP musi posiadać możliwość zaprogramowania wirtualnych bądź fizycznych przycisków zdarzenia RCP.

4. Dodatkowe informacje

Odporność SKD na próby nieautoryzowanego dostępu podnosi zastosowanie dedykowanego klucza kodowania czytników i kart. Rozwiązanie to jednak nie jest racjonalne w przypadku małych sądów, i budynków z małą liczba przejść, dlatego do rozważenia pozostaje np. wprowadzanie jednolitego rozwiązania w kilku budynkach podległych i komunikacja w L2 sieci , w budynkach, w których jest dużo wydawanych kart gości proponuje się wrzutnie kart dla gości opuszczających budynek, bądź nadawanie kodu EAN lub QR na dokumentach, wrzutnia może znajdować się przy ostatnim zabezpieczonym wyjściu np. w obudowie kołowrotka, bramki i działać jako czytnik RFiD.

optymalnym rozwiązaniem przy wdrażaniu SKD jest wykonywanie prac w oparciu o przygotowany projekt, jednakże dokumentacja powykonawcza jest niezbędnym minimum, które należy uzyskać od wykonawcy systemu.

SKD powinien być naprawiany na bieżąco, konserwowany i poddawany przeglądom technicznym nie rzadziej niż 1 raz w roku. Czynności te powinny być wykonywane przez przedsiębiorców posiadających odpowiednie certyfikaty producenta/ dystrybutora systemu. System powinien również przejść testy współdziałania w wymaganych obszarach

Po zainstalowaniu SKD, należy uzyskać od podmiotu instalującego system deklaracje zgodności z przyjętymi rozwiązaniami,.

5. Wymagania ogólne dotyczące systemu kontroli dostępu

Zgodnie z warunkami architektury oraz wymaganiami Użytkownika / inwestora w zakresie bezpieczeństwa budynku, projektowany system kontroli dostępu działający w oparciu o protokół internetowy IP oraz sieć Ethernet, kt6ry ma spełniać następujące funkcje oraz założenia uzgodnione z Użytkownikiem:

- System kontroli dostępu zaprojektowano w klasie stopnia ryzyka 2 w skali ad 2 do 4 zgodnie z norma PN-EN 60839-11:2014-01;
- liczbę i rozmieszczenie elementów systemu kontroli dostępu przyjęto na podstawie założeń projektowych. System zaprojektowano z myślą o maksymalnym bezpieczeństwie;
- Jeden kontroler ma obsługiwane tylko jedno przejście jednostronne lub dwustronne;
- Okablowanie do kontrolerów drzwi budowane jest zgodnie z normami wymienionymi w punkcie okablowania strukturalnego, tj. w konfiguracji gwiazdy i przy rygorze, ze łącza stale nie mogą przekroczyć długości 90 m dla połączeń w oparciu o medium miedziane;
- Okablowanie przeznaczone dla systemu kontroli dostępu rozprowadzane do kontrolerów ma być obsługiwane przez Główny Punkt Dystrybucyjny GPD oraz Piętrowych Punktów Dystrybucyjnych;
- Założono zastosowanie kontrolerów działających w sieci Ethernet;
- Do kontrolera do pracy w windzie montaż oraz podłączenie należy uzgodnić z dostawcą windy po wyborze dostawcy systemu.
- System ma posiadać budowę modułową oraz działanie on-line jak i offline;
- System ma posiadać architekturę klient - serwer;
- Kontroler ma być łączony w sieci poprzez Ethernet;
- Kontroler oraz osprzęt drzwiowy ma być zasilany poprzez dedykowany zasilacz 12V DC znajdujący się w obudowie kontrolera, bądź poprzez przełącznik sieciowy POE z buforem podtrzymania systemu min. 2godz
- Każdy kontroler ma posiadać podtrzymanie bateryjne przy braku zasilania;
- Kontroler ma posiadać własną pamięć i pracować bez polaczenia z serwerem, bądź siecią Ethernet, a po powrocie łączności zsynchronizować dane, przejście w tryb offline musi być sygnalizowane w aplikacji wartowniczej i zarządczej oraz zapisane w postaci LOG`u na serwerze.
- Oprogramowanie systemu ma być dostępne zarówno w wersji dedykowanego serwera z preinstalowanym systemem kontroli dostępu jak i w wersji do instalacji na innym sprzęcie spełniającym minimalne wymagania do jego uruchomienia w zależności od potrzeb użytkownika;
- Wersja oprogramowania ma być łatwo rozszerzalna wraz ze zwiększeniem się potrzeb użytkownika, wraz z modułami, spersonalizowanymi przez inwestora.
- System ma umożliwiać obsługę czytników biometrycznych, i kodów QR i EAN
- System ma mieć możliwość podłączenia czytników posiadających funkcje domofonu;
- System ma umożliwiać podział kontrolowanego obszaru na strefy i monitorowanie każdej z nich osobno;

- System musi posiadać rozbudowany moduł służący do zliczania liczby osób w danej strefie kontroli dostępu w celu łatwej i przejrzystej prezentacji listy osób aktualnie znajdujących

- System ma udostępniać funkcjonalność zarzadzania pojazdami, poprzez czytniki dalekiego zasiegu bądź system LPR

- System ma posiadać funkcje wizualizacji obiektu za pomocą map, oraz wizualizacje trybu alarmowego dla dodatkowych wejść i wyjść alarmowych dla np. czujnikow pir, kontaktronów itp.

- System ma posiadać możliwość raportowania czasu i obecności realizując Rejestrację Czasu Pracy;

- System ma posiadać funkcje zdalnego otwierania drzwi;

- System musi posiadać funkcje obsługi tagów RFiD i NFC

- System kontroli dostępu ma mieć możliwość programowego łączenia zdarzeń z różnych systemów oraz alarmowania o nich za pomocą przeznaczonej do tego aplikacji;

- System ma umożliwiać dodanie dodatkowych funkcji wraz ze zmianą potrzeb użytkownika:

- W systemie ma być zagwarantowana możliwość konfiguracji funkcji służy dla dowolnej liczby drzwi, stref, lokalizacji.

- System musi posiadać wbudowany moduł oprogramowania integrującego SMS (Security Management System).

6. Architektura systemu

Projektowany system topologicznie będzie w układzie gwiazdy, gdzie centralnym punktem będzie serwer, kolejnymi rozgałęzieniami będą przełączniki sieciowe i kontrolery systemu, każdy kontroler obsługiwał będzie jedno przejście chronione i będzie umiejscowiony w sposób jak najbardziej ograniczający dostęp do niego osób niepowołanych, a każda próba ingerencji będzie skutkowała alarmem sabotażowym, zarówno kontrolera jak i czytnika oraz okablowania strukturalnego. Okablowanie strukturalne należy wykonać w kat. 6A, gdzie wszystkie elementy toru będą objęte gwarancją producenta na okres 25 lat dla integralnego systemu. Łączność między przełącznikami będzie realizowana za pomocą światłowodu jednomodowego 12 włóknowego prefabrykowanego zakończonego w dedykowanej kasecie. Przełączniki muszą być zarządzalne i obsługujące Vlan oraz SFP+
Na system kontroli dostępu, na poziomie lokalnym, składają się następujące elementy:

- Oprogramowanie Serwer klienci
- Kontrolery przejścia
- Bramki kontroli dostępu
- Czytniki RFID z funkcja MFA
- Możliwość zastosowania w systemie czytników biometrycznych kodów QR i EAN
- Elementy wykonawcze jak elektro-zaczepy rewersyjne, zwory elektromagnetyczne, rygle itp. Każdorazowo uzgadniane z inwestorem, inspektorami, Państwową strażą pożarną, konserwatorem zabytków zarówno w ich zadziałaniu jako i sposobie montażu

Przyciski wyjścia awaryjnego

dostępowe karty zbliżeniowe

- Stanowisko wydawania kart

7. Multiplikacja systemu

Aplikacja zarządzająca musi zakładać funkcjonalność pozwalającą na zarzadzanie i integracje z lokalizacjami rozproszonymi posiadającymi połączenie poprzez sieć teleinformatyczną.

Cechy multiplikacji:

Możliwość zarzadzania i konfiguracji wieloma lokalizacjami z poziomu użytkownika z odpowiednimi uprawnieniami nadanymi przez Administratora Globalnego,

Wydawanie i kodowanie kart z dla wielu lokalizacji.

Konfiguracja dostępu użytkowników.

Tworzenie global

Możliwość raportowania zdarzeń wielu lokalizacji,

Przesyłanie alarmów do odpowiedniej grupy użytkowników

Raportowanie i zarzadzanie systemem kontroli czasu pracy, oraz ręczne generowanie raportów i plików wymiany dla ZSRK.

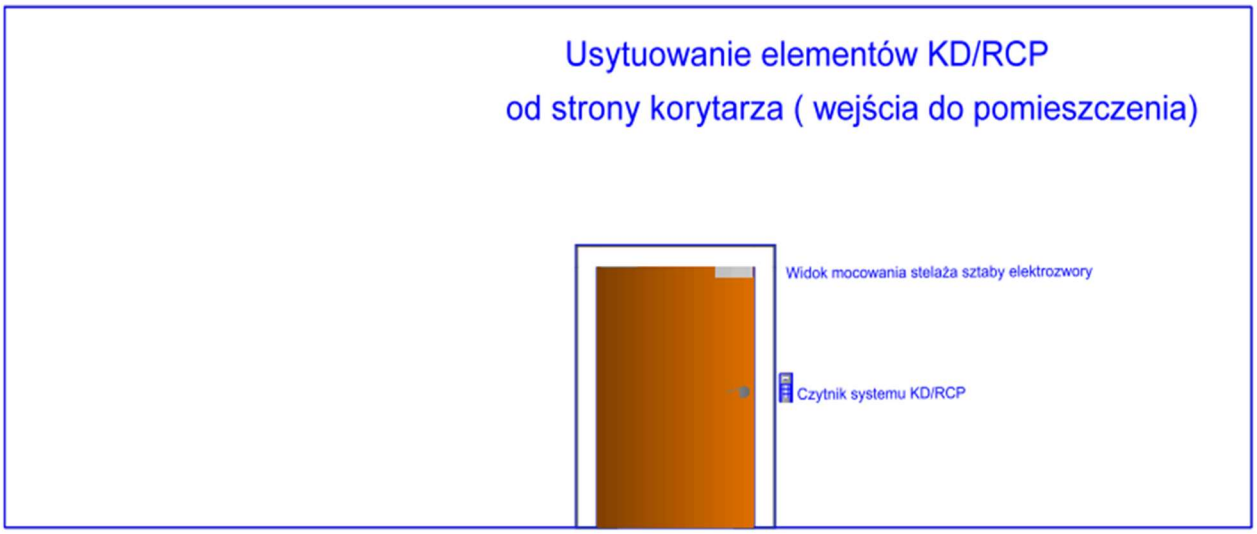
8. Centralny System Zaręczania

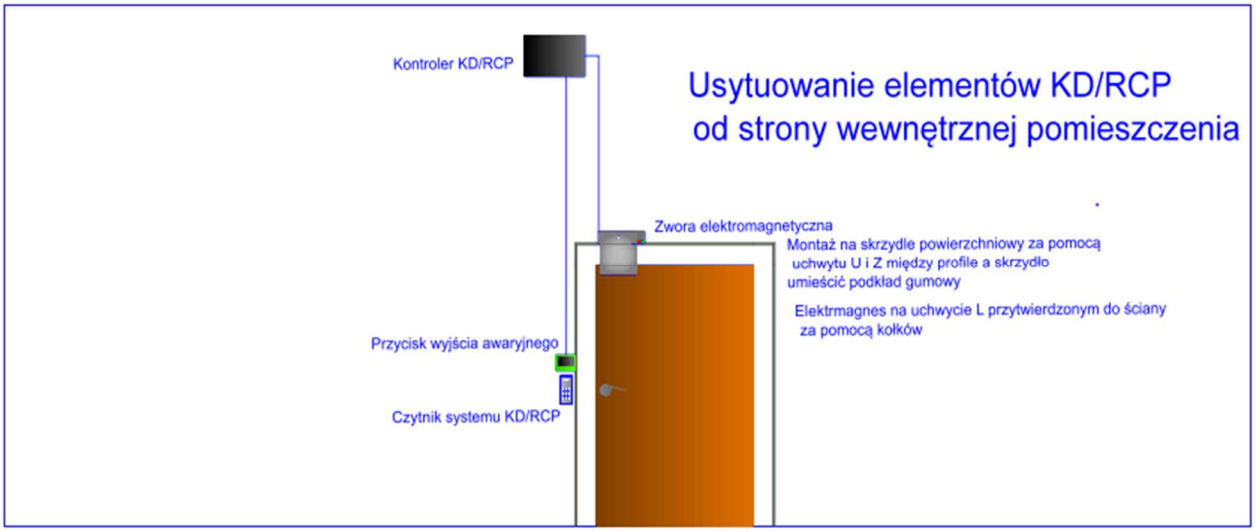
System kontroli dostępu może działać dla każdej lokalizacji niezależnie lub zostać skonfigurowany hierarchicznie z serwera centralnego.

9. *Drzwi wejściowe strefy kontrolowanej*

Drzwi strefy kontrolowanej obejmują wejścia do budynku oraz drzwi wejściowe do poszczególnych pomieszczeń (gabinety, archiwa, toalety).

W skład systemu drzwiowego wchodzą następujące elementy:





10. Czytniki kontroli dostępu

Czytniki kontroli dostępu powinny spełniać następujące wymagania:

- audiowizualna sygnalizację stanu drzwi (buzzer i/lub diody LED), np.gdy przełożymy kartę do czytnika aktywowany jest buzzer, gdy karta uprawniona dioda LED jest załączana na dłuższy czas (kolor zielony), gdy brak uprawnień do dioda czerwona i zielona mruga szybko - zabezpieczenie przed odwrotną polaryzacją styków zasilających.

- transmisja danych pomiędzy czytnikiem i kartą odbywać się ma po protokole Wiegand

- pracować jednocześnie na dwóch częstotliwościach 125KHz i 13,56 MHz

- odczytywać karty EM, HID oraz Mifare (ISO 14443A)

- posiadać indeks ochronny IP66

-mogą także dodatkowo dla celów RCP i szczególnych (według potrzeb inwestora) wyposażone być w dotykowy wyświetlacz TFT bądź LCD

11. Kontroler Przejścia

- praca w trybie sieciowym (ON-LINE) i autonomicznym (OFF-LINE) samodzielna praca kontrolerów SKD tj. bez komunikacji z serwerem, w oparciu o posiadane dane konfiguracyjne w pełnym zakresie funkcjonalnym, buforowanie i rejestracja w pamięci nieulotnej zdarzeń do momentu odzyskania komunikacji z serwerem

- wielkość bufora, co najmniej 100 000 zdarzeń w każdym kontrolerze

- pojemność identyfikatorów użytkowników nie może być mniejsza, niż 26 000 osób.

- obsługa protokołu odczytu Wiegand 26/34/66 bitów

- możliwość rozszerzenia o dodatkowe 4 wejścia i 4 wyjścia

Praca w trybie autonomicznym każdego kontrolera powinna zapewniać zachowanie w pamięci nieulotnej uprawnień w zakresie dostępu dla użytkowników, oraz pozostałych parametrów związanych z działaniem kontrolowanego przejścia.

Każdy kontroler winien być wyposażony w dualną pamięć umożliwiającą wykonanie synchronizacji danych kontrolera z serwerem bez konieczności blokowania urządzań SKD (drzwi, kołowrotów, szlabanów) i użytkowników. Np. uprawnienie są zmienione w locie (komunikacja IP) nie ma to odczuwalnego wpływu na pracę urządzenie, tj mogą być wykonywane operacje równolegle (identyfikacja karty, dodawanie uprawnień do tego samego kontrolera).

Jeden kontroler (sterownik) będzie obsługiwać maksymalnie jeden rodzaj przejścia.

Obudowa kontrolera (sterownika) powinna uniemożliwiać bezpośredni dostęp osobom nieuprawnionym.

Kontroler winien posiadać możliwość wyposażenia go w dodatkowe rozszerzenie alarmowe realizujące funkcję definiowanego alarmu manualnego, alarmu na obecność dymu bądź gazu w pomieszczeniu, alarmu sygnalizacji włamania oraz reakcji na alarm pożarowy. Płyta rozszerzeń musi posiadać co najmniej 4 wejścia oraz 4 wyjścia umożliwiające współpracę z innymi elementami.

Dodatkowo kontroler (sterownik) powinien posiadać możliwość czasowego otwierania drzwi dowolną kartą celem zebrania numerów kart i ich autoryzacji.

Kontrolery mają zapewniać realizację funkcji „anti-passback", która uniemożliwia ponowne otwarcie danych drzwi w zadeklarowanym odstępie czasu, bądź bez uprzedniego przejścia do następnej strefy oraz funkcję "śluza", która uniemożliwi otwarcie danych drzwi przed fizycznym zamknięciem innych drzwi

12. Bramki kontroli dostępu

1. Bramki dostępowe

Przy wejściach głównych do budynku w ciągach komunikacyjnych dostępnych dla petentów stosować bramki stanowiące fizyczna barierę ograniczającą swobodny dostęp do obiektu.

W tym celu należy zastosować bramki uchylne. Na obudowie bramek wejścia i wyjścia montować czytniki zbliżeniowe. W normalnym trybie pracy otwierana jest tylko jedna bramka (wejściowa lub wyjściowa). Przy wyborze bramek należy kierować się oprócz wskazanej funkcjonalności, względami estetycznymi tak aby kolor i wykonanie nawiązywały do elementów budynku, bramki powinny być w jak największym stopniu przezierne więc zaleca się konstrukcje ażurowe bądź szklane.

2. Obsługa niepełnosprawnych

W celu obsługa niepełnosprawnych na wózkach inwalidzkich bramki powinny posiadać funkcjonalność otwarcia dwóch skrzydeł w jednym kierunku. Do tego celu służy specjalna karta będąca w dyspozycji ochrony.

3. Integracja z SSP

W celu umożliwienia ewakuacji należy doprowadzić sygnał z systemu SSP w celu ewakuacyjnego otwarcia skrzydeł bramek (zgodnie z kierunkiem ewakuacji). Bramki będą posiadały możliwość swobodnego ręcznego odchylenia skrzydła.

13. *Specyfikacja techniczna elementów składowych systemu kontroli dostępu*

1. Serwer systemu

W projekcie zastosowano oprogramowanie systemu kontroli dostępu z baza danych zainstalowane na dedykowanym serwerze.. Z serwerem kontroli dostępu, poprzez sieci LAN połączone zostaną kontrolery typu A, B i RCP. Oprogramowanie serwera systemu KD zostanie zainstalowane na dedykowanym serwerze umieszczonym w pomieszczeniu serwerowni i spełniający minimalne wymagania sprzętowe przedstawione w poniższej tabeli serwer dostarczony będzie zamawiającemu

W trakcie realizacji projektu przez wykonawcę.

Tabela. Minimalne wymagania dla serwera KD

Nazwa	**Serwer kontroli** dostępu
System operacyjny	Windows server 2016 lub nowszy
Procesor	Intel Xeon
Pamięć RAM	16 GB RAM lub wiecej
Karta graficzna	zintegrowana
Pamięć minimalna	2x 500GB SSD (RAIDl)

2. Specyfikacja techniczna okablowania

Minimalna ilość żył do elementów (ilość elementów może być brany w zależności od elementów umieszczonych na rzutach przypisanych do danego przejścia):

- kontaktron - YTDY 6x0,5
- przycisk wyjścia roboczego (dotykowy) - YTDY 6x0,5;
- przycisk wyjścia rob. bezdotykowy - YTDY 6x0,5;
- przycisk awaryjny - LiYCY 2xl,O (przelotowo) + YTDY 6x0,5 (monitorowanie stanu);
- elektrozamek/rygiel/zwora magnetyczna - LiYCY 2xl,O;
- elektrozamek/rygiel/zwora magnetyczna z czujnikiem poleżenia drzwi - LiYCY 2xl,O + YTDY 6x0,5;
- elektrozamek z czujnikami poleżenia klamki, drzwi itp. - YTDY 8x0,5;

Zaleca się pozostawienia zapasu żył do wykorzystania w przyszłości lub awaryjnego, np. YTDY 8x0,5.

Rozszycie kabla powinno znajdować się w puszcze np. przycisku wyjścia lub awaryjnym, jednak chronionym przed łatwym dostępem osób trzecich, należy zawsze pamiętać o instalacji aby zachować estetykę pomieszczenia, oraz stanowisko komisję konserwatorską.

W razie konieczności bruzdowania, bruzda może naruszać jedynie strukturę tynku i warstw wierzchnich, w przedziale 15-20mm i głębokości do 20mm. Bądź podanej w pozwoleniu komisję konserwatorską dla projektu technicznego.

3. Przycisk wyjścia ewakuacyjnego

Przycisk stosowany na przejściach ewakuacyjnych lub w przypadku zastosowania zwory magnetycznej.

Przycisk posiada dwa styki - jeden do przerwania obwodu elektrycznego zamka; drugi styk do monitorowania stanu położenia przycisku. Przycisk montować powierzchniowo na kołki rozporowe.

4. Elektrozamek

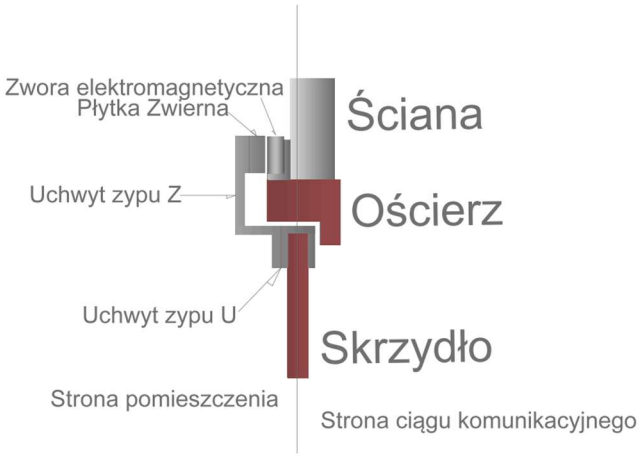
Stosować elektro zaczepy rewersyjne N O , bez pamięci i bez blokady.

W drzwiach p o ż a r o w y c h n a l e ż y zastosować element z dopuszczeniem do użycia w systemach pożarowych.

5. Zwora elektromagnetyczna z kontaktronem

Zwory elektromagnetyczne należy stosować we wszystkich drzwiach drewnianych i zabytkowych montaż każdorazowo należy uzgadniać z nadzorem konserwatorskim.

Należy zastosować zwory elektromagnetyczne 12V min. 280kg z kontaktronem. Rodzaj montażu dostosować do typu drzwi, w budynkach pod opieką komisję konserwatorską założyć można, iż wszystkie drzwi są zabytkowe i montaż nie może naruszać ich struktury, w założeniu zarówno do skrzydła jak i ościeży, należy wówczas wykorzystać element montażowy nie inwazyjny.



Propozycja montażu Zwory Elektromagnetycznej

Co do zasady należy przyjąć, że zworę należy montować ponad futryna (nie naruszając futryny) przy wykorzystaniu różnego typu uchwytów L, Z, I, U oraz ich odmian.

Zwory montować po stronie bezpiecznej zwykle wewnątrz pomieszczenia.

6. Karty zbliżeniowe

Tagi dostosować dla potrzeb użytkownika oraz kompatybilności z wykorzystanym systemem

7. Urządzenia dodatkowe

W przypadku montażu nowych drzwi Montaż elektrozamka dobór odpowiedniej listwy zaczepowej oraz zamka zatrzaskowego ustalić z producentem stolarki drzwiowej.

8. Zasilacze i obudowa

Zastosowane w projekcie zasilacze kontrolerów konwertują napięcie sieciowe 230 V na napięcie 12 V DC o prądzie dostosowanym do potrzeb elementów systemu. Zasilacz znajduje się w zamykanej na klucz, metalowej obudowie razem z kontrolerem, w której pozostawiono wolne miejsce na akumulator awaryjny. Zasilacz zapewnia zasilanie wszystkich urządzeń peryferyjnych podłączonych do kontrolera, a obudowa dodatkowo wyposażona jest w styk sabotażowy monitorowany przez wejście kontrolera. Wielkośc zasilacza który stanowi także obudowę kontrolera należy zawrzeć w przedziale 200-300mm krawędzi dolnej i 100-250 mm wysokości przy czym zachować montaż napowierzchniowy, przy użyciu kołków w przedziale fi 6-8mm i długości pomiędzy 40 a 80mm (nie używać kołków typu szybki montaż) zastosować można także kotwę chemiczną jednak jej użycie należy skonsultować z komisją konserwatorską.

14. Zasilanie instalacji

1. Zasilanie normalne sterowników kontroli dostępu zapewnić 230V z ogólnej cieci elektrycznej budynku, z rozdzielnic lokalnych.
2. Terminale RCP zasilić punktu dystrybucyjnego POE.
3. W sterownikach montować akumulatory podtrzymujące prace poszczególnych systemów.

15. Stanowisko ochrony

Stanowisko ochrony wyposażyć w stacje robocza umożliwiająca na monitoring zdarzeń w SKD ska w czasie rzeczywistym. Stanowisko powinno w sposób graficzny monitorować ruch i alarmy, dwa stanowiska znajdujące się w pomieszczeniu ochrony, a drugie w korytarzu, gdzie odbywa się kierowanie ruchem osobowym.

16. Stanowisko personalizacji kart

W lokalizacji ustalonej z zamawiającym zlokalizowane zostanie stanowisko do kodowania kart.

4. SYSTEM SYGNALIZACJI NAPADU I WŁAMANIA

Zgodnie z wymogiem inwestora zaprojektowano nowy system SSWiN dla kancelarii tajnej spełniające najnowsze standardy bezpieczeństwa.

1. Podstawy prawne opracowania, normy i wytyczne

Norma PD6662: 2003 Schemat zastosowań norm europejskich dla systemów sygnalizacji włamania
Norma EN50131-1:2003 Systemy alarmowe - Systemy włamaniowe. Wymagania og61ne (stopień 3)
Norma TS50131-3 Systemy Alarmowe- Systemy włamaniowe: część 3- Urządzenia sterujące i wskazujące (stopień 3)
Norma EN50131-6: 1998 Systemy Alarmowe - Systemy Włamaniowe - Zasilacze (stopień 3)
Norma EN50136 - 1 - 1: 1998r Systemy Alarmowe - Systemy Transmisji Alarmów - Wymagania og61ne dla systemów transmisji alarmów
Norma EN50136 - 1 - 3: 1998r Systemy Alarmowe - Systemy Transmisji Alarmów - Wymagania dla systemów wykorzystujących cyfrowe moduły komunikacyjne pracujące w publicznej sieci telefonicznej
CE
R&TTE 99/5/EC
BS 6799:1996

2. Opis systemu

Na rzutach przedstawiono miejsce instalacji elementów systemu SSWiN.

W projekcie przewiduje się centralę motowaną w pomieszczeniu kancelarii tajnej. Klawiatura do obsługi systemu będzie znajdowała się z zamykanej obudowie a przed wejściem będzie znajdować się sygnalizator optyczno-akustyczny. Dodatkowo w systemie zaprojektowano następujące elementy:

Ekspandery 8we./4wy.
Ręczny, przewodowy, przycisk napadowy, grade 3
Czujka inercyjna (sejsmiczna) - montaż na wybranych ścianach oraz szafach/sejfach, grade 3
Czujka zbicia szkła, grade 3
Czujka PIR + MW, antymasking, grade 3
Czujka zbicia szkła, grade 3
Manipulator (klawiatura)
Zewnętrzny sygnalizator optyczno-akustyczny, grade 3
Wewnętrzny sygnalizator optyczno-akustyczny, grade 3
Czujka zbicia szkła, grade 3
Czujka PIR + MW, antymasking, grade 3

3. *Wymagania dla systemu SSWiN*

Min 1000 użytkowników, oraz obsługa min 520 linii dozorowych
obsługa 32 niezależnych grup, podsystemów
obsługa 2 akumulatorów 18Ah/12V
interfejs wielojęzyczny EN.PL
4 niezależne magistrale systemowe pracujące w standardzie RS485 9600bit/s, transmisja full duplex, asynchroniczna
obsługa min 4 klawiatur dotykowych .
współpraca z systemowymi urządzeniami bezprzewodowymi.
moduł telekomunikacyjny do monitorowania systemu w standardzie SIA, DTMF, MICROTECH, CONTACT ID wbudowany na płytę lub jako moduł
możliwość współpracy centrali z siecią LAN/WAN za pośrednictwem interfejsu ETHERNET z wykorzystaniem protokołów TCP/IP *I* UDP wraz z szyfrowaniem transmisji oraz możliwością programowania modułu zapasowego w celu uzyskania toru transmisji rezerwowej
możliwość współpracy z GSM/ GPRS
możliwość przejścia z magistrala na światłowodu przy użyciu standardowego konwertera.
możliwość wizualizacji oraz sieciowania central przy użyciu protokołu komunikacyjnego
możliwość weryfikacji alarmów wbudowanym torem audio
wbudowany nadzorowany zasilacz typ A o wydajności min 2,5A w tym l A d1a akumulatora.
Nadzorowane stany (prąd pobierany z zasilacza, napięcie, akumulator, sieć 230V, bezpieczniki - wszystkie stany muszą być dostępne z poziomu dowolnego manipulatora LCD podpiętego do systemu)
wyjścia zasilania 2 kpl 12V *I* 0,75A - poziom tetnieri <50mV
pob6r prądu centrali 150mA
obsługa linii dozorowych pracujących w standardzie 3EOL oraz 4EOL - w celu bezpośredniej obsługi antymaskingu oraz wyjść diagnostycznych podpinanych do systemu urządzeń
dl 440mm, szer. 352mm, wys. 90.
waga 6,4kg
temperatura pracy od -10 do +55 stopni

5. Okablowanie Strukturalne

1. *Podstawa opracowania projektu*

Podstawą do opracowania zagadnień związanych z okablowaniem strukturalnym są normy okablowania strukturalnego.

Normy europejskie dotyczące og61nych wymagań oraz specyficznych dla środowiska biurowego:

- PN-EN 50173-1:2018 Technika informatyczna - Systemy okablowania strukturalnego - część 1: Wymagania og61ne.
- PN-EN 50173-2:2018 Technika informatyczna - Systemy okablowania strukturalnego - część 2: Pomieszczenia biurowe.
- IEEE P802.3bt-2018 Standard for Ethernet Amendment 2: Power over Ethernet over 4 Pairs.
- ISO/IEC 11801:2017 - Information technology-Generic cabling for customer premises specifies.

Wykonawca ma obowiązek wykonać instalacje okablowania zgodnie z wymaganiami opisanymi w dokumentacji projektowej, a jeśli którykolwiek z dokumentów normalizacyjnych uległ aktualizacji wg nowych aktualnych wymagań.

Uwaga:

W przypadku powołań normatywnych niedatowanych obowiązuje najnowsze wydanie cytowanej normy.

2. *Wymagania ogólne dotyczące okablowania strukturalnego*

- okablowanie strukturalne budowane jest zgodnie z w/w normami, tj. w konfiguracji gwiazdy i przy rygorze, ze łącza stale nie mogą przekroczyć długości: 90 m;
- wszystkie elementy pasywne składające się na okablowanie strukturalne muszą być oznaczone nazwa lub znakiem firmowym, tego samego producenta okablowania i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu 25-letniej gwarancji udzielonej bezpośrednio przez w/w producenta;

  ilość i rozmieszczenie gniazd przyjęto na podstawie informacji podanych przez użytkownika; w trakcie realizacji, ostateczna lokalizacja gniazd logicznych w pomieszczeniach (bez zmiany ich ilości) powinna być ustalona pomiędzy Użytkownikiem, a Wykonawcą;
- minimalne wymagania elementów okablowania dla transmisji danych pod względem wydajności to Kategoria 6a (komponenty)/ Klasa EA (podstawowa wydajność całego systemu) i zapewnienie możliwości transmisji l0 Gigabit Ethernet 802.3an;
- okablowanie przeznaczone dla systemu kontroli dostępu obsługiwane będzie przez szafę dystrybucyjną
- okablowanie poziome ma być prowadzone podwójnie ekranowanym kablem typu F/FTP kat. 6A w powłoce zewnętrznej LSZH, klasa CPR B2ca;
- wszystkie kable okablowania poziomego mają być zakończone w osprzęcie połączeniowym zgodnie z norma PN-EN 50173-1;
- aby zagwarantować i potwierdzić wymagania wydajności komponentów okablowania miedzianego dla transmisji danych komponenty przeznaczone do zabudowy (gniazda, kable krosowe) muszą posiadać certyfikaty wydane przez akredytowane niezależne laboratoria(np. GHMT, Delta) potwierdzające zgodność systemu/komponentów z wymaganiami normy międzynarodowej, tj. ISO/IEC 11801 lub EN50173-1 minimum klasy EA;
- dla okablowania poziomego należy zastosować proste panele krosowe o wysokości l U, niezaładowane, na 24 oddzielne moduły ekranowane;
- punkty końcowe systemu oparte zostały na ekranowanych modułach RJ45 kat..s; umieszczonych w obudowach kontrolerów systemu kontroli dostępu:

na całość zainstalowanego okablowania ma być udzielona gwarancja bezpośrednio przez producenta na okres minimum 25 lat;

środowisko wewnątrz budynku, w którym będzie instalowany osprzęt kablowy, jest środowiskiem biurowym i zostało ono sklasyfikowane, jako M1I1C1E1 zgodnie z norma PN-EN 50173-1; maksymalne długości kanałów transmisyjnych okablowania poziomego zostały obliczone dla najgorszego przypadku wzrostu temperatury otoczenia, tj. do 40°C;

3. *Wymagania dla kabli symetrycznych*

1. Wymagania dla ekranowanych kabli symetrycznych F/FTP kat.6A

Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o

maksymalnej średnicy zewnętrznej 7,01 (co determinuje maksymalną średnicę żyły na 23 AWG). Nie dopuszcza się kabli o większej średnicy zewnętrznej, instalacja ma być poprowadzona ekranowanym kablem konstrukcji F/FTP z osłona zewnętrzna trudnopalna (LSZH).

Minimalne wymagania dla kabla miedzianego F/FTP kategoria 6A:

- Średnica zewnętrzna kabla- max. 7,01 mm;
- Przekr6j żyły przewodnika- 23 AWG;
- Rodzaj osłony zewnętrznej: LSZH;
- Euro klasa - B2ca-s1a,d1,al;
- Gwarancja pełnego wsparcia PoE i zgodności z wymaganiami IEEE 802.3af i IEEE 802.3at, IEEE 802.3bt dla aplikacji PoE i PoE+;
- Temperatura pracy: -20°C do +60°C;
- Temperatura podczas instalacji: 0°C do +50°C;
- Zgodność z ISO 11801 Kategoria 6A/Klasa EA, ANSI/TIA-568-C.2;
- Zgodność z IEC 60332-1, 60754-2, 61034-2, 60754-2;
- Certyfikat zgodność normatywnej niezatężanego laboratorium dla min. 4 połączeń w kanale do lOOm dla ISO 11801 Kategoria 6A/Klasa EA;
- Pozytywne parametry w zakresie częstotliwości do min. 500MHz;

kabel F/FTP kat.6A 4/23AWG 82ca LSZH

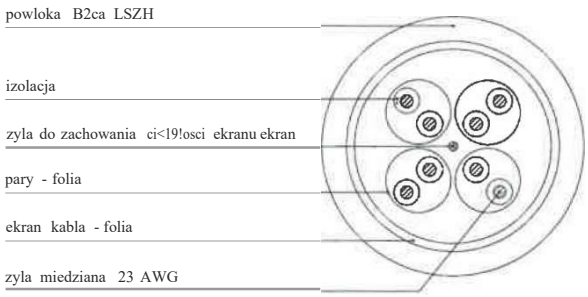


Tabela 1. Wymagania dla kabla (F/FTP kat.6A)

OGOLNE DANE TECHNICZNE	
Budowa kabla	F/FTP (zgodnie z rysunkiem)
Wydajność kabla	Klasa EA wg. ISO/IEC 11801
Kategoria kabla	6A
Średnica zewnętrzna kabla	max. 7,01 mm
Średnica przewodu	min. 1,168 mm
Grubość płaszcza	min. 0,635 mm

Przekrój żyły przewodnika	23AWG
Rodzaj osłony zewnętrznej	LSZH
Wag a	48,514 kg/km
PARAMETRY ELEKTRYCZNE	
Rezystancja niezrównoważenia DC	2%
Rezystancja prądu stałego DC	max. 7,61 ohms na 100 m
Pojemność wzajemna	max. 4,2 nF na 100 m przy 1 kHz
NVP	80%
częstotliwość	500 MHz
Maksymalne napięcie robocze	aov
PARAMETRY SRODOWISKOWE	
Temperatura pracy	-20°C do +60°C
Temperatura podczas instalacji	0°C do +50°C
Klasa odporność ogniowej - Euro klasa wu, EN50575	B2ca
Wydzielanie dymu wg. EN50575	sla
Wydzielanie płonących kroili/czastek we, EN50575	dl
Wydzielanie kwasów wg. EN50575	al

Tabela 2. Wymagania parametrów transmisji przy częstotliwościach kluczowych

częstotliwość	Tłumienie	PS NEXT	RL
[MHz]	[dB]	[dB]	[dB]
100	17,9	78,4	27
250	28,6	74,3	19
500	41,1	67,1	15,2
650	47,1	63,5	12,4

6. SYSTEM REJESTRACJI CZASU PRACY (RCP)

1. Cel systemu rejestracji czasu pracy

Projektowany system RCP ma za zadanie zautomatyzować w możliwym stopniu, dział kadrowo-płacowy Inwestora, dane z systemu RCP będą zbierane w postaci bazy danych i synchronizacja jej z bazą danych systemu ZSRK. System będzie rozróżniał wiele zdarzeń z kategorii kadrowo płacowych nie tylko wejścia i wyjścia ale również delegacje, wyjścia „awaryjne" prywatne itp.

2. Architekturasystemu rejestracji czasu pracy

System będzie bazował na zdefiniowanych makrach z uwzględnieniem różnych tytułów nieobecności. RCP ma możliwość zdefiniowania wielu systemów pracy w ramach przepisów zawartych w normach prawnych, oraz regulaminach wewnętrznych.

System ma współpracować z zaprojektowanym urządzeniem rejestrującym zdarzenia odpowiadające rozpoczęciu i zakończeniu pracy, oraz na podstawie rejestrów i ręcznie dopisanych zdarzeń w aplikacjach klienckich ma wyliczać czas pracy poszczególnych osób. Rejestracja czasu pracy oparta jest na dostępne funkcjonalności użytego terminala wyposażonego w ekran dotykowy oraz czytnik kart, umieszczonego w pomieszczeniu komunikacji na parterze w niedalekiej odległości od głównego wejścia do budynku. Terminal będzie zainstalowany na ścianie w wyznaczonym miejscu. użyty terminal jest składowym elementem architektury systemu kontroli dostępu Systemy KD i RCP będą umożliwiały konfigurację z poziomu jednego interfejsu, co ułatwi zarzadzanie systemami oraz tworzenie między nimi logicznych zależności. Do zliczania pierwszego i ostatnie odbicia w dniu pracy będą wykorzystywane również: czytniki KD zlokalizowane na wejściu do budynku (np. bramkach) a sam dotykowy terminal będzie wykorzystywany do rejestracji niestandardowego opuszczenia budynku np. wyjście służbowe w godzinach pracy.

Weryfikacja pracowników będzie się odbywała z wykorzystaniem kard zbliżeniowych KD. Możliwe będzie również dodatkowe zabezpieczenie hasłem, System po zarejestrowaniu autoryzacji będzie zapisywał czas zdarzenia (rozpoczęcie pracy, zakończenie pracy) oraz na ich podstawie obliczał czas pracy. Poza tym będzie istniała również możliwość zdefiniowania innych typów wyjść, np. wyjście służbowe/prywatne/normalne/inne.

3. Wymagania ogólne dla systemu rejestracji czasu pracy

Projektowany system RCP musi spełniać następujące wymagania::

- System rejestracji czasu pracy ma działać jako integralana część systemu kontroli dostępu:
- System będzie posiadał wspólną architekturę z systemem KD, systemy będą połączone w jednej sieci TCP/IP;
- Zdarzenia będą zapisywane na serwerze kontroli dostępu oraz w lokalnej pamięci kontrolerów KD;
- Czas pracy będzie kalkulowany na podstawie odbić na terminalach lub na podstawie informacji wprowadzanych manualnie przez pracowników;
- System ma umożliwiać wyszukiwanie nieprawidłowości (np. brak odbicia karta po zakończeniu pracy, niezwrócony klucz);
- System ma mieć funkcje wyboru typu wejście/wyjście;
- System ma umożliwiać zapis wyjść służbowych, prywatnych, normalnych czy innych.

4. *Funkcjonalność terminala systemu rejestracji czasu pracy*

Użyty terminal umożliwia konfigurację przycisków funkcyjnych w trybie pracy „czas i obecność", Prawidłowe działanie umożliwi użytkownikowi po przyłożeniu karty zbliżeniowej zobaczenie listy z zdefiniowanymi typami wejść i wyjść. Po wybraniu dedykowanej i dostępnej dla danego użytkownika opcji następuje rejestracja.

Zgromadzone informacje takie jak czas rozpoczęcia i zakończenia pracy, imię i nazwisko użytkownika, stanowisko pracy z zadanego przedziału czasowego, wybranego urządzenia oraz obejmującego konkretna grupę, wcześniej zdefiniowanych, posiadaczy kart można wygenerować w wybranym formacie plików.

Na podstawie otrzymywanej ewidencji czasu pracy pracowników można monitorować spóźnienia, nadgodziny i nieobecności co znacznie ułatwia prowadzenie miesięcznych rozliczeń placowych,

5. *Terminal rejestracji czasu pracy*

W celu rejestracji czasu pracy w projekcie zastosowano inteligentny terminal z wyświetlaczem dotykowym z funkcja wyboru typu wejście/wyjście (stuizbowe/prywatne /normalne/inne). Wielofunkcyjny, inteligentny terminal dostępowy zapewnia najwyższy stopień zabezpieczenia. Terminal powinien charakteryzować się przejrzystym menu dostępnym po autentykacji dla każdej z grup zaszeregowania i strefy, terminale w różnych lokalizacjach będą wymieniały informacje gdy pracownik jednej z lokalizacji zostanie oddelegowany do innej. Terminal będzie dawał możliwość wyboru trybu wyjścia oraz zapewniał możliwość weryfikacji wieloskładnikowej. Komunikacja w systemie RCP będzie odbywała się za pomocą protokołu TCP/IP, a w razie utraty łączności kontroler przejdzie w tryb offline zapewniając zapis do 50 000 zdarzeń, które będą automatycznie zsynchronizowane po odzyskaniu polaczenia z systemem, system natomiast powiadomi wybranego użytkownika o utracie komunikacji i konieczności sprawdzenia bądź interwencji serwisu. Czytnik aby realizować założenia trybu autentykacji złożonej wypozasony będzie w czytnik RFID ,klawiaturę oraz opcjonalnie w czytnik biometryczny o minimum 5 sygnaturach dla jednego użytkownika

Posiada złącze Ethernet 100 Mbps oraz komunikuje się bezpośrednio z serwerem systemu kontroli dostępu,

Najważniejsze cechy terminala:

- Ekran dotykowy LCD o przekątnej 4,3";
- intuicyjny interfejs graficzny użytkownika;
- informacje konserwacyjne / inteligentny punkt ochrony;
- Czytnik i kontroler Ethernet w jednym urządzeniu:
- Narzędzie do zdalnego programowania umożliwiające pobieranie nowego oprogramowania;
- Cztery wejścia analogowe do monitorowania stanów alarmowych oraz dwa wyjścia przekaźników do aktywowania rygla zamka drzwi i/lub innych urządzeń:
- Baza danych offline niemszcząca do 200 000 rekordów posiadaczy kart oraz do 50 000 transakcji offline;
- Obsługa szerokiej gamy technologii inteligentnych kart;

- Zasilanie PoE/PoE+.

Specyfikacjatechniczna

Terminal z wyświetlaczem dotykowym zastosowany do rejestracji czasu pracy w projekcie znajduje się zgodnie z podkładami dołączonymi do projektu. Zasilanie terminala będzie zapewnione za pomocą PoE/PoE+. Do kontrolera doprowadzony będzie przewód symetryczny skrętkowy 4 - parowy o parametrach przewidzianych w dokumentacji projektowej okablowania strukturalnego. W tabeli poniżej przedstawiono minimalne wymagania dla terminala.

Tabela. Specyfikacja techniczna terminala

Parametry fizyczne	
Wymiar	35-65mm podstawy dolnej x 100-200mm wysokości
Waga kontrolera	< 450g
Obudowa	Ognioodporny poliwęglan zapewniający całkowicie zamknięty w środku układ elektroniczny.
Wyświetlacz LCD	Pojemnościowy, dotykowy o przekątnej 4,3", 480*272 piksele, kolorowym, 16-bitowym
Zasilanie	
Napięcie	10-14 V DC
Pobór prądu	350 mA (typowo), 500 mA (max) - zasilanie PoE (brak możliwości zasilenia elementów peryferyjnych - np. elektrozamka) 350 mA (typowo), 500 mA (max) - zasilanie PoE+ (850 mA dostępnych dla urządzeń peryferyjnych - np. elektrozamka)
Środowiskowe	
Temperatura pracy	-20° to 70°C - PoE -25° to 55°C - PoE+
Stopień ochrony IP	IP65
Funkcjonalność	
Przełączalne wyjścia	2x FET 12Vdc (1.6A na dwa wyjścia), 2x 30V 2A (wyjścia „suche")
Wyjścia	2 przekaźniki, styki beznapięciowe
Wejścia dodatkowe	Cztery wejścia, sabotażu:
Pamięć	128 MB RAM, 256MB NANO Flash
Obsługiwane technologie kart	MiFARE (CSN)/ DESFire (CSN)/ CEM DESFire/ iCLASS/ iCLASS SE
Bateria zapasowa RTC	3,0V akumulator litowo-jonowy
Pamięć użytkowników	do 250 000 użytkowników w trybie offline
pamięć zdarzeń	do 50 000 operacji w trybie offline
Interfejsy komunikacyjne	
Czytniki	RS485, polaczenia za pomocą zacisków śrubowych
Serwer	10/100BaseT TCP/IP kat.5 UTP RJ45
Tryby pracy	Tryb drzwi, Śluza, Tryb przed drzwiowy, RCP, Globalny PIN, PIN jako karta, Posterunek
Regulacje	FCC Part 15, CE, UL 294

7. SYSTEM SYGNALIZACJI POZARU

Przedmiotem opracowania jest projekt przetargowy instalacji teletechnicznych: system detekcji pożaru w budynkach Sądu Okręgowego.

1. Podstawa opracowania:

Podstawę opracowania stanowią:

- Zlecenie wykonania projektu przetargowego instalacji SSP
- Rzuty projektu architektonicznego
- Przepisy i normy branżowe
- Ustalenia międzybranżowe

2. Podstawa opracowania:

Niniejszy projekt przetargowy obejmuje swoim zakresem:

- Opis systemu sygnalizacji pożaru
- koncepcje prowadzenia instalacji
- lokalizacje urządzeń

3. Podstawa opracowania:

- Ustawa o ochronie przeciwpożarowej (Dz. U. nr.81 poz.351 z dn.24.08.1991) ze zmianami.
- Rozporządzenie MSWiA z dn. 11 czerwca 2010 w sprawie ochrony przeciwpożarowej budynków i innych obiektów budowlanych i terenów (Dz.U. nr 109 z dnia 22.06.2010 r., poz. 719)
- Rozporządzenie Ministra infrastruktury z dn. 12.04.2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. Nr 75 z dn. 15.06.2002r.).
- PKN-CEN/TS 54-14:2020 Systemy sygnalizacji pożarowej. Projektowanie, zakładanie, odbiór, eksploatacja i konserwacja instalacji
- Podręcznik projektanta systemów sygnalizacji pożarowej- CNBOP 2013r.

4. Charakterystyka obiektu

Projekt przetargowy przewiduje demontaż istniejących instalacji SSP (bez okablowania) w budynkach SO. Budynki zostaną objęte całkowitą ochrona Systemem Sygnalizacji Pożaru.

ochrona za pomocą automatycznych czujek pożarowych nie objęto następujących przestrzeni:

- pomieszczenia mokre, małe pomieszczenia sanitarne
- pustki budowlane, w której nie znajdują się żadne instalacje elektryczne lub teletechniczne

Projekt zakłada wykorzystanie istniejącego okablowania po zdemontowanych czujkach (o ile okablowanie będzie zgodne z wymaganiami producenta systemu) w celu zmniejszenia ingerencji w ścianach zabytków, dlatego dopuszcza się stosowanie czujników bezprzewodowych z komunikacją dwukierunkową i dających możliwość jednoznacznej identyfikacji w systemie jak ma to miejsce w przewodowych systemach adresowalnych, czujniki prócz stanu alarmowego muszą sygnalizować konieczność wymiany baterii, wszystkie zastosowane czujniki musza być multisensorowe aby zmaksymalizować stopień detekcji pożaru. Wrazie wymiany czujników o ile umiejscowienie spełnia wymagania techniczne i formalne nowy czujnik zainstalować w miejscu demontowanego detektora.

5. Wymagania dla systemu bezpieczeństwa

Zgodnie z wytycznymi projektu architektonicznego i wymaganiami w zakresie bezpieczeństwa przeciwpożarowego budynków system sygnalizacji pożaru spełniał będzie następujące funkcje:

- Umożliwienie automatycznego przekazania sygnału do centrum monitoringu PSP - dostawa i montaż w gestii inwestora (WYMAGANE)
- Dwustopniowe alarmowanie po detekcji pożaru- czasy muszą być dostosowane do kubatury obiektu oraz obsady.
- Wczesne wykrycie źródła potencjalnego pożaru z dokładny wskazaniem jego miejsca na wyświetlaczu centrali bądź wyniesionego panelu obsługi
- Wyłączenie urządzeń wentylacyjnych i klimatyzacyjnych jeżeli występują lub w przyszłości)
- Zamkniecie klap pożarowych w kanałach wentylacyjnych (jeżeli występują lub w przyszłości)
- Automatyczne sterowanie urządzeniami ochrony przeciwpożarowej

Monitorowanie klap p-poz. na instalacji wentylacji i klimatyzacji ,

- Wysterowanie windy (jeżeli występuje lub w przyszłości)
- Zwolnienie przejść ewakuacyjnych wyposażonych w instalacji kontroli dostępu
- System posiada czujki, dla których w łatwy sposób będzie można sprawdzić poziom ich zabrudzenia, np. poprzez urządzenie serwisowe leczące się z czujkami za pomocą podczerwień bądź automatycznie generowanemu raportowi ze stanu

6. Opis ogólny systemu, lokalizacja urządzeń

W niniejszej instalacji zaprojektowano system oparty na adresowalnych centralach alarmowych. Centrala pracuje w układzie linii pętli dozorowych z możliwością indywidualnego adresowania wszystkich elementów na pętlach, oraz obsługująca protokoły czujników bezprzewodowych

W skład systemu będą wchodziły następujące elementy:

- Centrala z wyświetlaczem LCD i panelem obsługi
- Adresowalne czujki multisensorowe optyczno-temperaturowe
- Ręczne ostrzegacze pożarowe (ROP)
- Moduły wejść/wyjść (monitorująco-sterujące)
- Sygnalizatory optyczno-akustyczne z synchronizacją
- Adaptery czujników bezprzewodowych
- Bezprzewodowe czujniki multisensorowe

Linie dozorowe w konfiguracji pętli wraz z izolatorami zwarć zapewniają wysoka odporność systemu na uszkodzenia linii dozorowej. Elementy pętlowe (czujki, ROPy, moduły typu quad) posiadają wbudowane izolatory zwarć.

1. Lokalizacja urządzeń systemu sygnalizacji pożarowej

Projekt przewiduje lokalizacje podstawowych urządzeń systemu w następujących miejscach:

- Centrale systemu sygnalizacji pożarowej w pomieszczeniach ochrony, serwerownie. bądź innym bezpiecznym miejscu natomiast panel wyniesiony obsługi w miejscu ciągłego przebywania, osób np. wartownie, pomieszczenia monitoringu itp
- Czujki optyczne zostały rozmieszczone na rzutach zgodnie z przepisami pożarowymi
- Czujki punkotowe optyczno-temperaturowe umieszczone zostały aby zmaksymalizować proces wykrywania zagrożenia, szczególnie w archiwach gdzie wykorzystywane są regały przesuwne.
- Ręczne ostrzegacze pożarowe umieszczone przy wyjściach ewakuacyjnych z kondygnacji i z budynku; na każdym piętrze klatek schodowych, według norm zalecających ich rozmieszczenie na drogach ewakuacyjnych.
- Moduły sterująco-monitorujące - zlokalizowane w pobliżu tych urządzeń

Wszystkie czujki zainstalowane w przestrzeni sufitu podwieszanego, w przestrzeniach o ograniczonym dostępie projektuje się ze wskaźnikami zadziałana umieszczonymi bezpośrednio na suficie podwieszanym lub na ścianach w pobliżu. W chwili wykrycia pożaru czujka przekazywać będzie sygnał do centrali jak również jej zadziałanie będzie sygnalizowane przez wskaźniki zadziałania. Dla czujek montowanych ponad sufitem podwieszanym pełnym, należy przewidzieć rewizje dostępowa,

Lokalizacja centrali z wyświetlaczem LCD powinna zapewniać, aby:

- do CSSP był Łatwy dostęp dla straży pożarnej;
- wskaźniki i manipulatory b y ł y łatwo dostępne dla straży pożarnej oraz osób odpowiedzialnych za obiekt;
- natężenie oświetlenia było takie, aby można było łatwo dostrzec i odczytać sygnatury wizualne;
- poziom tła akustycznego był na tyle mały aby słyszalne były sygnały alarmowe i ostrzegawcze centrali
- środowisko było czyste i suche;
- możliwość uszkodzenia mechanicznych sprzętu było niewielkie;
- ryzyko powstania pożaru b y ł o niewielkie, a miejsce zabudowy centrali było dozorowane, przez co najmniej jedna czujkę należącą do instalacji sygnalizacji pożarowej nadzorowanej przez te CSP.

Centrala sygnalizacji pożarowej, lub panel wyniesiony służący do obsługi systemu, powinny być montowane w strefie, w której stale przebywają ludzie i w sposób ciągły nadzorowana przez odpowiednio przeszkoloną obsługę.

W pomieszczeniu, w którym zostanie zainstalowana centrala sygnalizacji pożarowej, należy umieścić:

- plan sytuacyjny nadzorowanego obiektu;
- opis funkcjonowania i obsługi urządzeń sygnalizacji pożarowej tzw. Instrukcje stanowiskową wraz z numerami do SMA oraz serwisu.
- wskazówki, jak należy postępować w przypadku pożaru:
- książkę eksploatacji i konserwacji instalacji SSP, w której należy wpisywać:
  - przeprowadzone kontrole instalacji;
  - przeprowadzane naprawy;
  - zmiany i uzupełnienia instalacji;
  - wszystkie alarmy z podaniem daty, godziny i przyczyny ich wywołania.

Książkę taka należy prowadzić również: w przypadku, gdy centrala sygnalizacji pożarowej jest wyposażona w pamięć zdarzeń.

7. Opis działania systemu

Elementy pętlowe, zainstalowane w adresowalnej pętli dozorowej, po odebraniu właściwego sygnatur z centrali (adresu elementu), przesyłają zwrotne sygnatury z informacją o swoim rodzaju i stanie. Wymiana informacji miedzy elementami pętlowymi i centrala odbywa się poprzez procesory pętli dozorowych zainstalowane na płycie głównej centrali lub kartach pętlowych. Po analizie odebranych sygnałów, mikroprocesor centrali informacje te przetwarza i wypracowuje odpowiednie sygnały dla pozostałych układów.

Realizując zaprogramowane procedury działania, układ steruje poprzez magistrale przekaźnikami lub liniami sygnałowymi, wyświetlaczem LCD, elementami sygnalizacyjnymi oraz obsługowymi paneli wyświetlacza i obsługi na drzwiach centrali.

Dla transmisji informacji pomiędzy centrala a adresowalnymi urządzeniami na pętlach dozorowych, wykorzystywany jest protokół pętlowy przekazujący do centrali wszystkie parametry w postaci analogowej. Pozwala to na prace czujki w różnych trybach wykrywania pożaru, dobieranych w trakcie programowania pod kątem optymalizacji czułości iminimalizacji ryzyka alarmów fałszywych. W czujkach wielosensorowych wszystkie sensory mogą pracować jednocześnie, zaś oprogramowanie uwzględnia zależności pomiędzy ich parametrami.

Zasilacz sieciowy ma za zadanie dostarczenie roboczego napięcia centrali, a w razie braku zasilania sieciowego role źródła zasilania pełni rezerwowa bateria akumulatorów podtrzymujących prace w czuwaniu na 72h.

8. Opis urządzeń

1. Centrala Sygnalizacji Pożaru

Central dobrana do użycia w systemie musi cechować się prostotą obsługi, łatwością instalacji oraz przejrzystością komunikacji stanów systemu na ekranie LCD swoim bądź panelu wyniesionego.

Wszystkie te funkcje stały się możliwe do realizacji dzięki zastosowaniu architektury wieloprocesorowej z funkcją samo-diagnozowania i koordynowaną przez 32-bitowy procesor. System zapewnić najwyższy poziom niezawodności, szybkość reakcji, łatwość użytkowania, prostotę połączenia, możliwość dodania dodatkowych modułów i elastyczność. W centralach powinny zostać wykorzystane między innymi następujące technologie: komunikacja redundantna pętli, technologia sieciowania central, technologia Emergency54 oraz technologia Janus.

Centrala powinna mieć 5 nadzorowanych wyjść do sygnalizacji alarmów i usterek (sprawność tych wyjść jest stale monitorowana). Centrala może wykryć i zdiagnozować anormalne warunki i zapewnia szerokie spektrum wizualizacji sygnałów: alarm, prealarm, usterka, wczesne ostrzeganie, wyłączenie, test, monitorowanie. Cały stan systemu pokazywany jest zarówno na diodach LED jak i na wyświetlaczu graficznym. Oprócz nadzorowanych wyjść centrala posiada min. 2 przekaźniki do sygnalizacji alarmu i usterki, a także wyjście sygnalizacji wyłączenia akumulatora.

W celu zwiększenia liczby wejść i wyjść w centrali można dołączyć moduł rozszerzeń IN/OUT. Każdy z terminali IN/OUT można skonfigurować do pracy albo jako nadzorowane wejście albo nadzorowane wyjście lub też jako strefa zawierająca czujniki konwencjonalne. Te konfigurowalne na 3 sposoby terminale usuwają

nieelastyczność występującą w konwencjonalnych modułach rozszerzeń wejść/wyjść a także umożliwiają zarządzanie strefami składającymi się z konwencjonalnych detektorów. Poprzez szynę RS485 zapewniane jest dołączenie terminali wyniesionych w systemie min.2 sztuki.
Poprzez szynę RS485 możliwe powinno być także podłączenie i zarządzanie modułami sterowania gaszeniem.
Systemy adresowalne zgodnie z normami PN-EN 54-2 i PN-EN 54-7

Parametry techniczne i główne funkcje central:
• Adresowalna centrala przeciwpożarowa
• 2 pętle z możliwością rozszerzenia do 8 pętli dla modeli
• Centrala zgodne z normą PN-EN54-2
• Struktura wieloprocesorowa
• Główny CPU - 32 bitowy
• Architektura umożliwiająca sieciowanie redundantne
• Obsługa komunikacji awaryjnej (redundancja CPU)
• Możliwość zarządzania 30 centralami w sieci token–ring poprzez moduł sieciowy.
• Łatwy zdalny dostęp poprzez moduł LAN
• 2 lub 4 przewodowe połączenie urządzeń w pętli
• Obsługa do 240 urządzeń w pętli
• Możliwość zarządzania do 8 terminali wyniesionych połączonych poprzez szynę RS485, maksymalna odległość pomiędzy centralami to 1000m
• Zarządzanie modułami sterowania gaszeniem poprzez szynę RS485
• 24 V źródło zasilania dla urządzeń zewnętrznych
• 24 V resetowalne wyjście
• Przekaźnik do odłączania akumulatorów przy dużym rozładowaniu
• RS232 i USB do ściągania/wysyłania danych
• Bufor na 2000 zdarzeń
• Samo-wprowadzanie (dla urządzeń w pętli)
• Samo-adresowanie (dla urządzeń w pętli)
•Możliwość podłączenia czujników konwencjonalnych (poprzez moduł IN/OUT)
•Duży, podświetlany, alfanumeryczny wyświetlacz do zarządzania/użytkowania
• Klawisze nawigacyjne do łatwego dostępu do funkcji wyświetlanych graficznie
• Klawisze szybkiego dostępu (Ewakuacja, Wycisz, Reset, Weryfikacja, Test)
• Brzęczyk (zapewniający sygnały dźwiękowe), sygnalizacja uszkodzeń i alarmów
• Przyjazne dla użytkownika oprogramowanie (działa pod Windows)
• Kod lub klucz do funkcji 2 poziomu (zgodnie z normą PN-EN54-2)
• Złącze na płycie centrali do podłączenia sondy termicznej
• Testowanie wydajności akumulatorów
• Metalowa obudowa
• Główne zasilanie 230V AC ± 10%
• Miejsce na dwa akumulatory 17Ah, 12V, bądź zasilacz zewnętrzny z akumulatorami o większej pojemności

2. Czujniki multisensorwe

Czujnik multisensorowe to czujnik dymu i temperatury wykorzystujący najnowsze technologie wykrywania. Stąd jego zwiększona niezawodność dla wszystkich typów pożarów (zwłaszcza dla szybko palących się płynów łatwopalnych, które wyzwalają niewielkie ilości dymu) czego rezultatem jest niezwykle duża odporność na fałszywe alarmy. Czujka może być ustawiona do pracy w trybie, który najbardziej pasuje do aplikacji już na obiekcie aby dostosować ją d zmiennych śrdowiskowych.

• Tryb Dualny (domyślny) – czujnik wyzwoli alarm kiedy zmierzona wartość przekracza ustawiony próg czułości na dym, lub gdy mierzona wartość temperatury przekracza ustawiony próg. Dodatkowo w przypadku nagłego wzrostu temperatury czułość detekcji dymu ustawiana jest na maksimum. Ten tryb charakteryzujący się wysoką czułością pozwala na wykrywanie pożarów o wysokiej temperaturze (np. pożary płynów łatwopalnych jak np. alkoholu)
• Tryb OR: czujnik wyzwoli alarm kiedy zmierzona wartość przekracza ustawiony próg czułości na dym, lub gdy mierzona wartość temperatury przekracza ustawiony próg. Ten tryb charakteryzuje się dyskretną analizą czułości pozwalającą na wykrycie pożaru z wysoką emisją dymu i niskim poziomem temperatury (np. materiały tlące się) jak również pożary z niską emisją dymu oraz wysoką temperaturą (np. palące się materiały chemiczne).
• Tryb AND: czujnik wzbudzi alarm tylko kiedy oba progi czułości : dymu i temperatury są przekroczone w tym samym czasie. Ponieważ jest to tryb obniżonego działania należy uwzględnić wszelkie czynniki
ryzyka zanim wybierze się ten tryb pracy czujnika.
• Tryb DYM: wyłączany jest detektor temperatury i czujnik pracuje jak zwykły sensor optyczny dymu.
• Tryb TEMPERATURA: czujnik działą jak zwykły czujnik termiczny bądź termo-rózniczkowy.

Najwcześniejsza z możliwych sygnalizacja pożaru dzięki:

- zastosowaniu technologii wielosensorowej,
- wyposażeniu każdej czujki w mikro-procesor (rozproszona inteligencja),
- inteligentnemu połączeniu niezależnych metod detekcji (bardzo szerokie pasmo detekcji),
- wysokiej odporności na zwarcia i przerwy w obwodzie.

Optymalne zabezpieczenie przed fałszywymi alarmami dzięki:

- rozproszonemu mechanizmowi podejmowania decyzji o alarmie,
- minimalnej podatności na zakłócenia elektromagnetyczne automatycznej adaptacji do środowiska.

Wysoka niezawodność eksploatacyjna i niskie koszty konserwacji dzięki:

- ciągłej autodiagnostyce,
- możliwości zdalnej diagnostyki,

Niski koszt instalacji i wysoka elastyczność dzięki:

- zastosowaniu technologii pętli dozorowej ,
- możliwości wyłączania sensorów przez funkcję czasową lub zdarzenia w systemie.

3. Gniazda czujek

Czujki będą być instalowane w gniazdach dedykowanych o różnej budowie w zależności od miejsca montażu np. o podwyższonej odporności na wilgoć, itp. Gniazdo dzięki swojej konstrukcji zapewnia utrzymanie ciągłości pętli dozorowej nawet w przypadku demontażu czujki. Pozwala to na sprawne uruchomienie i dokonanie pomiarów elektrycznych pętli dozorowej jeszcze przed zamontowaniem urządzeń.

4. Wskaźnikzadziałania

Wskaźnik zadziałania służy do sygnalizowania uruchomienia detektora pożarowego. W ten sposób możliwa jest szybka lokalizacja aktywowanej czujki, gdy wskaźnik LED na urządzeniu jest niewidoczny. Stosowanie wskaźników zadziałanie projektuje się dla czujek zamontowanych nad sufitem podwieszanym, podniesioną podłogą techniczną itp.

M4

5. Ręczny ostrzegacz pożarowy

Ręczne ostrzegacze pożarowe posiadać certyfikat zgodności z PN-EN 54 – 11 i dopuszczenie CNBOP Ręczne ostrzegacze pożarowe oraz PN-EN 54 – 17 Izolatory zwarć.

Dane techniczne:

Napięcie zasilania 19-30 VDC – nominalnie 24 VDC

Temperatura pracy od - 10 ° C do + 55 ° C

Dopuszczalna wilgotność względna (bez kondensacji) 95% RH

Wymiary (WxSxG) 84 x 84 x 45 mm

Stopień ochrony IP30

Masa 126 g

Ze względu na zniwelowanie kosztów i skomplikowania ubsługi zaleca się oprzeć system o tzw. ROP-y kasowalne, gdzie alarm kasuje się za pomocą klucza a nie wymiany szybki.

6. Modułów Wejśc/Wyjść

Moduł Pętlowy umożliwia komunikację central adresowalnych z urządzeniami zewnętrznymi za pomocą jego wejść i wyjść w zależności od modelu który to określa liczbę i rodzaj wejść i wyjść. Wejścia powinny być wejściami nadzorowanymi poprzez rezystor końca linii, i mogą być wykorzystane do sprawdzania stanów urządzeń jak klapy p.poż, zasilacze, centrale oddymiania itp. Wyjścia bez potencjałowe nadzorowane, wykorzystane mogą być np. do sterowania zwalnianiem systemów KD oraz badaniem ciągłości linii, natomiast wyjścia potencjałowe do sterowania i badania ciągłości linii sygnalizatorów. Moduł należy umieścić w dedykowanej obudowie o wymiarach 80-150mm podstawy i 80-150 wysokości i montować napowierzchniowo, przy użyciu kołków rozporowych.

7. Elementy systemu bezprzewodowego

W pomieszczeniach i ciągach komunikacyjnych gdzie występują sztukaterie, zdobienia i stropy wymuszające ingerencje projektuje się system bezprzewodowy, oparty o translatory komunikacyjne i czujniki bezprzewodowe wielosensorowe z komunikacja dwukierunkowa

1. Translator

Podłączony do pętli systemu detekcji pożaru translator przetwarza komunikaty i stany otrzymane z bezprzewodowych czujników, modułów, wyzwalaczy itp. i raportuje wszystkie pozyskane informacje do centrali SAP. Dzięki pełnej komunikacji translator i wszystkie urządzenia bezprzewodowe rozpoznawane są w centrali SAP jako adresowalne elementy pętli.

Translator:

• wykorzystuje algorytm dynamicznej zmiany częstotliwości
• charakteryzuje się wysoką odpornością na szumy
• zapewnia stworzenie w pełni adresowalnego bezprzewodowego systemu detekcji pożaru
• oferuje możliwość podłączenia do 32 urządzeń bezprzewodowych
• może być programowany przy pomocy komputera PC
• jest prostym i ekonomicznym sposobem na rozszerzenie tradycyjnych systemów detekcji pożaru

Cechy i zalety urządzenia:

• komunikacja dwukierunkowa (urządzenie nadawczo-odbiorcze)
• zakres częstotliwości 868 MHz (zgodne z normą ETSI EN 300-220-1)
• modulacja FSK
• wielokanałowość (do 7 kanałów)
• automatyczne zarządzanie mocą transmisji
• dwie, prostopadłe do siebie anteny zapewniające bezpieczną i bezawaryjną komunikację
• zasilanie z pętli systemu detekcji pożaru
• natychmiastowa transmisja sygnałów alarmu, komunikatu błędu oraz zabezpieczenia (niepowołanej ingerencji) z podłączonych urządzeń bezprzewodowych

Dane techniczne:

zasięg komunikacji z urządzeniami podrzędnymi 200 m*
zasięg komunikacji z ekspanderami 500 m*
częstotliwość robocza 868-870 MHz
rodzaj modulacji FSK
kanały robocze 7

zasilanie z pętli głównej
prąd Imax = 25 mA
temperatura pracy -30°C…+55°C

2. Czujnik

Bezprzewodowa czujka wielosensorowa (optyczna i ciepła) musi być urządzeniem w pełni adresowalnym, kompatybilnym bezprzewodowymi translatorami i ekspanderem.
Czujka przeznaczona do pracy w przestrzeni otwartej i łączy w sobie zalety dwukanałowej czujki optycznej oraz czujki ciepła. Użyte algorytmy detekcji przy zachowaniu niewielkiej ilości fałszywych alarmów wykorzystanie sprawdzonych, adaptacyjnych algorytmów przetwarzania sygnałów radiowych
powinien zapewnić najwyższy poziom bezpieczeństwa i niezawodności systemu.
Cechy i zalety urządzenia:
• zaprojektowane zgodnie z normami
EN54-5, -7, -25 oraz EN54-29
• dwie diody LED zapewniające lepszą
sygnalizację alarmu
• zaawansowana,układ komory dymowej
• wewnętrzne przetwarzanie algorytmów
optymalizujące wydajność czujki
• kilka progów czułości czujki
• 8-letni czas pracy na komplecie baterii
• wykorzystuje standardowe i tanie baterie
litowe, które są w pełni monitorowane
• dwukierunkowa komunikacja bezprzewodowa
• kompatybilne z wszystkimi translatorami i ekspanderami
• zewnętrzna zakładka identyfikująca czujkę
• gwarancja 5 lat
Dane techniczne:
obliczeniowy zasięg
komunikacji min. 200 m*
częstotliwość robocza 868-870 MHz
max. moc
emitowanego sygnału <25mW
robocze kanały komunikacyjne 7
wybór progów czułości
3 dla części
optycznej,
2 dla cieplnej

9. Organizacja alarmowania

W czasie normalnej pracy stan systemu sygnalizowany jest na panelu obsługi centrali oraz Paneli Wyniesionych za pomocą odpowiednich kontrolek oraz wyświetlacza LCD.

W chwili zadziałania czujki wywołany zostaje alarm pożarowy I stopnia, który sygnalizowany jest akustycznie i optycznie na panelu centrali przez czas T1. W czasie T1 obsługa jest zobowiązana do potwierdzenia przyjęcia alarmu wciśnięciem przycisku wyciszenia. Jeżeli w czasie T1 (180 sekund czas taki spowodowany jest obszarem budynku oraz składem osobowym ochrony fizycznej) alarm I stopnia nie zostanie potwierdzony centrala automatycznie wejdzie w II stopień alarmu.

Potwierdzenie przyjęcia alarmu powoduje rozpoczęcie odliczania czasu T2 (180 sekund) przeznaczonego na dokonanie rozpoznania czy alarm jest uzasadniony. Po czasie T2 centrala wejdzie w II stopień alarmowania, chyba że wcześniej alarm zostanie skasowany.

W każdej chwili istnieje możliwość natychmiastowego wywołania alarmu poprzez wciśnięcie jednego z przycisków pożarowych rozmieszczonych w obiekcie lub przycisku EWAKUACJA na panelach obsługi.

Wejście centrali w stan alarmu II stopnia powoduje że zostaną uruchomione sygnalizatory akustyczne oraz nastąpi wysterowanie modułów sterujących odpowiedzialnych, za sterowanie urządzeniami ochrony pożarowej, zabezpieczanie dróg ewakuacyjnych, zatrzymanie wentylacji mechanicznej wprowadzenie wind w tryb zjazdu pożarowego.

Wywołane zostaną również zgodnie z opracowanym dla budynku scenariuszem pożarowym następujące akcje:

1. W przypadku powstania pożaru wszyscy zobowiązani są podjąć działania w celu jego likwidacji:

- zaalarmować niezwłocznie, przy użyciu wszystkich dostępnych środków osoby będące w strefie zagrożenia,

- wezwać straż pożarną.

2. Wezwanie straży pożarnej odbywa się za pośrednictwem nadajnika alarmowego UTA.

3. Przystąpić niezwłocznie, przy użyciu miejscowych środków gaśniczych do gaszenia pożaru i nieść pomoc osobom zagrożonym w przypadku koniecznym przystąpić do ewakuacji ludzi i mienia. Należy czynności te wykonać w taki sposób aby nie doszło do powstania paniki jaka może ogarnąć ludzi będących w zagrożeniu, które wywołuje u ludzi ogień i dym. Panika może być przyczyną niepotrzebnych i tragicznych w skutkach wypadków w trakcie prowadzenia działań ratowniczo gaśniczych. Dlatego prowadząc jakiekolwiek działania w przypadku powstania pożar należy kierować się rozwagą w podejmowaniu decyzji. Do czasu przybycia straży pożarnej kierowanie akcją obejmuje kierownik zakładu pracy /właściciel obiektu/ lub osoba najbardziej energiczna i opanowana.

Sposób ewakuacji i mienia określa instrukcja bezpieczeństwa pożarowego dla każdej z lokalizacji.

10. Montaż instalacji i prowadzenie okablowania

Montaż: wykonywać zgodnie z obowiązującymi w kraju normami i przepisami.

Uwagi odnośnie montażu okablowania i urządzeń:

- Celem uniknięcia kolizji zaleca się przeprowadzenie montażu instalacji SSP po wykonaniu innych instalacji w obiekcie, lub koordynować ich wykonanie na bieżąco z innymi branżami.
- Polaczenia pętli dozorowych detekcyjnych wykonać kablem dwużyłowy ekranowanym typu YNTKSYekw 2x1mm podtynkowo lub w rurkach bez halogenowych, korytach lub listwach instalacyjnych bez halogenowych. Sposób układania przyjąć taki sam jak dla instalacji elektrycznych zachowując zgodność z certyfikatem kabla.
- Obwody linii modułowych (sterujących), które wymagają podawania sygnału w czasie pożaru, wykonać kablem HDGs PH90 i HTKSH PH90-ilosc żył i przekrój pojedynczej żyły uzależniony od podłączanych urządzeń i odległości. Zespoły kablowe musza posiadać dopuszczenie do zastosowań przeciwpożarowych, przytwierdzonych bezpośrednio do podłoża, zgodnie z certyfikatem kabla, dla trasy E-90.
- W trasach kablowych o podtrzymaniu funkcji E-90 nie wolno układać innych kabli niż te, z którymi dana trasa kablowa została przebadana i potwierdzona odpowiednim atestem.
- Nad trasami kablowymi E-90 nie mogą przebiegać inne trasy, przewody, kanały (sanitarne, wentylacyjne itp.), kt6re nie poosiadają podtrzymania funkcji E-90 w czasie pożaru,
- Czujki instalować zawsze bezpośrednio na stropie lub suficie podwieszonym, jednak zwrócić uwagę na możliwość wystąpienia poduszki powietrznej.
- Czujki zaleca się łączyć w podanej (rosnącej) kolejności numeracji.
- Podczas montażu sprawdzać numerację oraz nazwy pomieszczeń. Dane te są niezbędne do wykonania opisu tekstowego w centrali. Nazwy pomieszczeń, ich numerację oraz nazwy stref określać w porozumieniu z Zamawiającym (Użytkownikiem). W trakcie montażu zaleca się nanosić numer seryjny urządzenia (adres) na dokumentacje w celu ułatwienia jego opisu i programowania.
- Moduły pętlowe instalować w miejscach umożliwiających przegląd i konserwacje,
- W przypadkach kolizji lub zbliżeń zachować odległość 50 cm czujek od ścian, podciągów, przewodów wentylacyjnych (o ile przebiegają one w odległości mniejszej niż 15 cm od stropu), opraw świetlnych itp.
- Zachować odległość czujek min. 1,5 m od kratek wentylacyjnych nawiewu i 0,5m od wywiewu.
- Zachować odległość min. 30 cm przewodów instalacji SSP od innych przewodów i kabli elektrycznych.
- Początki i końce linii dozorowych prowadzone w częściach pionowych instalacji prowadzić w osobnych trasach, przy czym dopuszcza się stosowanie wspólnej trasy dla początków i wspólnej dla końców linii pętlowych,

- Ręczne ostrzegacze pożarowe instalować na wysokości 1,5-1,7 m od podłogi, Sposób montażu natynkowo lub podtynkowo określa Komisja konserwatorska.
- Centrale sygnalizacji pożarowej posiadająca panel wyświetlacza i obsługi zainstalować na wysokość umożliwiającej łatwy odczyt informacji z jej pola odczytowego za pomocą kołków montażowych o Fi miedzy 8 a 12 mm i długości między 60 a 100mm

11. Zasilanie podstawowe i awaryjne

1. Centrala SSP zasilanie podstawowe

Projekt zakłada zasilanie podstawowe central SSP napięciem 230 VAC z wydzielonego pola dedykowanej rozdzielni, sprzed wyłącznika głównego prądu - doprowadzenie zasilania zgodnie z projektem elektrycznym.

UWAGA! Do obwodu zasilającego CSP nie wolno przyłączać innych odbiorników energii elektrycznej. Pole podłączenia zasilania oznaczyć napisem „CENTRALA SSP".

Połączenie kablowe wykonać jako nierozłączne, kablem energetycznym ognioodpornym z oddzielnym zabezpieczeniem w rozdzielni dla każdej z central CSP. stosować odpowiednie zasady ochrony przeciwporażeniowej.

2. Centrala SSP Zasilanie awaryjne

Projekt przewiduje zastosowanie central SSP wyposażonych w zasilanie akumulatorowe zapewniające prace przez 72h dla stanu czuwania i 0,5h dla stanu alarmu. Na tej podstawie obliczono minimalną pojemność baterii na 40 Ah

Czas 72h można obniżyć do 30h, pod warunkiem podpisania umowy serwisowej z odpowiednim czasem reakcji (w ciągu 24h) oraz zabezpieczeniem niezbędnych części zamiennych np. zasilacza do centrali pożarowej przez firmę serwisującą lub inwestora.

8. M o n t a ż urządzeń i prowadzenie przewodów

1. Montaż bramek i systemu przyzywowego

1. Montaż bramek

Do przeprowadzenia okablowania do bramek uchylnych należy dokonać zdjęcia okładziny posadzki oraz wykonać bruzdowanie pod rurę karbowana o przekroju pozwalającym przeprowadzić przewody z zapasem co najmniej 30%, a następnie odtworzyć posadzkę każdorazowo odtworzenie uzgodnić i wykonać pod nadzorem komisji konserwatorskiej w razie nie możliwości użycia pierwotnych materiałów . Dopuszcza się montaż kontrolera w obudowie bramek i przeprowadzenie od niego czytników systemu KD/RCP. Bramki osadzić na kotwach metalowych lub według zaleceń producenta. Zasilanie doprowadzić według wskazań producenta i zgodnie z nimi zabezpieczyć.

2. Montaż systemu przyzywowego

Jako system towarzyszący projektuje się system przyzywowy, w celu wezwania pomocy w razie problemów medycznych w pomieszczeniach sanitarnych. System ten ma za zadanie zaalarmowanie wyznaczonych osób o potencjalnym zagrożeniu życia, dopuszcza się użycie systemu bezprzewodowego. Każde z pomieszczeń powinno być wyposażone w przycisk przywoławczy przy drzwiach oraz przycisk cięgnowy przy toalecie. Powiadomienie może odbywać się poprzez zapalenie lampki nad drzwiami, bądź tablicy synoptycznej i pagera.
Tablica synoptyczna musi jednoznacznie wskazywać miejsce powstania zdarzenia.
Tablicę synoptryczną zamontować na kołki w pomieszczeniu ochrony, podobnie elementy przyzywowe.

2. Montaż kontrolerów i czytników

Montaż kontrolerów każdorazowo należy konsultować z komisją konserwatorską, jeżeli montaż wskazany w projekcie jest niemożliwy (np. kolizje z innymi instalacjami), dopuszcza się niewielkie przesuniecie urządzenia w celu obejścia kolizji. Kontroler należy zabezpieczyć przed dostępem osób niepowołanych.

Czytniki systemu KD/RCP należy montować, aby w jak największym stopniu ich powierzchnia stykała się z powierzchnią miejsca montażu. Do zamontowania należy użyć materiałów pozwalających trwale związać czytnik z miejscem montażu tak aby utrudnić jego zdjęcie przez osoby nie powołane, zaleca się użycia kołków rozporowych o fi między 6-8 mm a długości 40-80mm nie dopuszcza się użycia kołków typu szybki montaż.

Czytniki należy dobrać kolorystycznie, aby były jak najbardziej neutralne.

3. *Prowadzenie instalacji.*

1. Instalacja pozioma i pionowa

1. Instalacje systemu SSP

Instalacja systemu sygnalizacji pożaru dzieli się na dwie grupy:
- przewody i trasy pętli dozorowych wykonywane są z przewodów uniepalnionych YNTKSYekw 1x2x0,8mm I traktowane są jak trasy teletechniczne nie posiadające wedle norm odporności ogniowej, trasy takie prowadzone będą podtynkowo w bruzdach o wymiarach 35x20mm naruszających tylko warstwę okładziny ściany, którą trzeba odtworzyć według zalecenia komisję konserwatorską i materiałami posiadającymi odpowiednie atesty , na uchwytach plastikowych, bądź napowierzchniowo w rurkach RL16mm przytwierdzonych uchwytkami zamykanymi, bądź kanałach kablowych plastikowych, montaż taki sugerowany jest dla tras nad sufitami podwieszanymi. Do kotwienia uchwytów, aby zniwelować ubytki powstałe podczas wiercenia kotwę (kołek) należy jeżeli to możliwe wpuścić w fugę między materiały konstrucyjne, bądź użyć gwoździarek aby uszkodzenie powierzchniowy było możliwie najmniejsze.
- przerwody i trasy linii alarmowych i urządzeń wykonawczych, są trasami wykonywanymi w klasie ogniowej min. E60 choć zwykle przyjmuje się normę E90. Przewody prowadzone są podtynkowo w bruzdach i przytwierdzane na atestowane kotwy i uchwyty, każdorazowo bruzdowanie należy odtworzyć według zalecenia komisję konserwatorską i materiałami posiadającymi odpowiednie atesty.
Do kotwienia uchwytów, aby zniwelować ubytki powstałe podczas wiercenia kotwę (kołek) należy jeżeli to możliwe wpuścić w fugę między materiały konstrukcyjne, bądź użyć gwoździarek aby uszkodzenie powierzchniowy było możliwie najmniejsze.

2. Instalacja KD i sieci strukturalnej

Okablowanie dla systemu KD i LAN układane będzie podtynkowo bruzdach o wymiarach 40x20mm z naruszeniem tylko wierzchniej okładziny (tynk, gładź, farba) i mocowane do elementów konstrukcyjnych za pomocą uchwytów plastikowych, dopuszcza się, montaż obu instalacji w jednej bruździe. Drugim sposobem prowadzenia instalacji jest montaż powierzchniowy, w takim przypadku użyć możemy rurek RL montowanych w uchwytach zamykanych, kanałów kablowych plastikowych. Prowadzenie tras w miejscach pozbawionych okładzin należy wykonać napowierzchniowo z użyciem rurek RL bądź kanałów kablowych, elementy należy każdorazowo mocować do fugi tak aby zminimalizować uszkodzenie materiały konstrukcyjnego bądź przy użyciu gwoździarek.

3. Zasady ogólne

Podstawową zasadą, która należy przyjąć jest jak najmniejsza ingerencja w strukturę konstrukcji budynku, dlatego przyjmuje się za dopuszczalne uszkodzenie przy prowadzeniu tras jedynie wierzchniej warstwy ścian i stropów bez ingerencji w konstrukcję, każdorazowo po dokonaniu bruzdowania ścianę należy odtworzyć do stanu pierwotnego, jeżeli zachodzi potrzeba także całościowo pomalować, aby miejsca prac były niewidoczne. Trasy poziome należy prowadzić w ścianach zachowując odległość między 30 a 35 cm od styku ściany i stropu uważając przy tym na pozostałe instalacje oraz elementy konstrukcyjne budynku.
Podczas prac montażowych elementów mających swoje posadowienie na posadzce, jeżeli konieczne jest bruzdowanie, należy odtworzyć okładzinę posadzki materiałami odzyskanymi bądź identycznymi zaakceptowanymi przez komisję konserwatorską. W trakcie prowadzenia tras kablowych w szczególności podczas zastępowania starych elementów systemu nowymi jak to ma miejsce w przypadku np. czujników systemu SSP a niemożliwości wykorzystania startego okablowania należy wykorzystać, uprzednie trasy kablowe.

9. Bramki wykrywające metal

1. Bramka

Bramki wykrywające wnoszenie przedmiotów metalowych należy dostosować do szerokości ościeża drzwi przy, których będą umiejscowione, bramka musi w razie detekcji powiadomić sygnałem dźwiękowym i świetlnym o tym fakcie.

2. Funkcje dodatkowe

Dodatkowo bramki powinny być wyposażone w funkcję detekcji podwyższonej temperatury aby wyeliminować możliwe zagrożenie epidemiologiczne dla osób przebywających w budynku, fakt dokonania takiej detekcji powinien być zgłoszony odrębnym sygnałem.

3. Integracja

Bramki detekcyjne mogą być zintegrowane z systemem KD i zliczać ruch osobowy w budynku, który może być porównany w systemie z ilością wydanych kart dla petentów.

10. Kancelaria tajna

1. Wytyczne projektowania

Podstawową wytyczną do projektowania systemów bezpieczeństwa jest ustawa art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) oraz ZARZĄDZENIE MINISTRA SPRAWIEDLIWOŚCI z dnia 23 stycznia 2014 r. w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. Urz. MS poz.32).
W myśl tych aktów prawnych poza systemem SSP, projektuje się także system KD, SSWiN oraz CCTV

1. System SSP

System sygnalizacji pożarowej obejmował będzie detekcję, wystąpienia pożaru w klasie A, przetwarzanie sygnałów alarmowych odbywa się w Centrali Systemu Pożarowego i sygnalizowane jest na wyświetlaczu centrali i paneli wyniesionych.

2. System KD i SSWiN

Aby uniemożliwić dostęp do pomieszczeń przetwarzania informacji niejawnych, projektuje się system kd zintegrowany z systemem SSWiN. Wejście i rozbrojenie alarmu odbywać się będzie przy pomocy uwierzytelniania wielkoskładnikowego (RFiD + pin, Biometryka + Pin, Biometryka + RFiD), system uniemożliwi dostęp przez zainstalowanie elementów ryglujących w klasie pożarowej i wytrzymałości nacisku 2000 kg. Kontroler systemu Kd zintegrowany z systemem SSWiN i obsługujący czujniki PIR/WM, Czujnik Obecności, i czujnik otwarcia na każdym otworze okiennym i drzwiowym. Uprawnieniami zarządzał będzie jedynie wybrany administrator najwyższego zaszeregowania, a ruch nie będzie widoczny w systemie monitorowania Online. Urządzenia jak i instalacja wykonana będzie w min kat. Grade 3 a zasianie w Typie A.

3. System CCTV

System dozoru wizyjnego będzie lokalny i nie udostępniony nigdzie w obrębie sieci teleinformatycznej, uprawnienia do jego obsługi będą posiadały jedynie osoby z odpowiednimi uprawnieniami, System składał się będzie z Rejestratora NVR wyposażonego w 2 4TB dyski przeznaczone do pracy ciągłej, zintegrowany switch POE wyjście D-SUB oraz HDMI, możliwość pracy w sieci (opcja podłączenia). Kamery systemu CCTV będą kamerami w obudowie zintegrowanej o odporności 10J na uderzenia mechaniczne i IP65 na kurz i wilgoć. System CCTV prócz nagrań bieżących rejestrował będzie także, nagrania alarmowe dzięki integracji z KD/SSWiN, tj. każdorazową nieuprawnioną, próbę wejścia czyli użycie nieprawidłowego składnika autentykacji, próba taka zostanie zapisana w zdarzeniach alarmowych a obsługa zostanie o niej powiadomiona, poprzez wyświetlenie komunikatu na monitorze do tego przeznaczonym, informacje z monitoringu wizyjnego przechowywane będą min. Przez okres 30dni.