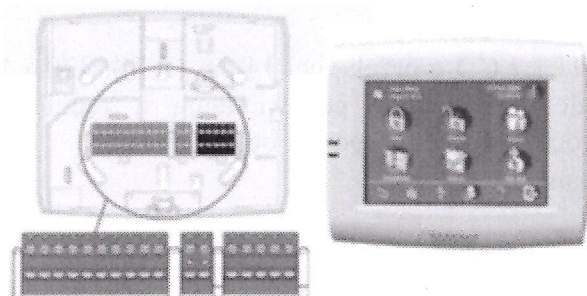


Sterowanie manipulatorem LCD



Parametry użytkowe:

- Ekran dotykowy - 14 cm (5,7") LCD z regulowanym podświetleniem LED
- Interfejs graficzny (16-bitowa paleta barw przy rozdzielczości 320 x 240 pikseli) składający się z intuicyjnych ikon i menu
- Wersje językowe do wyboru przez użytkownika
- Wbudowany głośnik z regulowaną głośnością
- Brak odsłoniętych części przy dostępie do zacisków; okablowanie w podstawie dołączane do zacisków wciskanych

Panel sterowania posiada głośnik generujący następujące sygnały:

- Sygnał naciśnięcia właściwego przycisku: potwierdzenie dokonania wyboru poprzez naciśnięcie obrazu na ekranie dotykowym.
- Sygnał niewłaściwego wyboru: wskazanie naciśnięcia nieaktywnego przycisku lub pola bez obrazu przycisku.
- Sygnał opóźnienia wejścia: powiadomienie o rozbrojeniu systemu w zaprogramowanym czasie.
- Sygnał opóźnienia wyjścia: powiadomienie o przygotowaniu do uzbrojenia systemu w zaprogramowanym czasie.
- Sygnał alarmu włamaniowego: wskazanie warunku alarmowego.
- Sygnał nadzoru włamaniowego: wskazanie warunku nieprawidłowości (problemu) nadzorowanego punktu.
- Sygnał problemu włamaniowego: wskazanie warunku nieprawidłowości (problemu) punktu.
- Gong: wskazanie uaktywnienia punktu.
- Sygnał problemu systemowego: wskazanie warunku problemu systemowego w rodzaju awarii sieci energetycznej.

Elementy regulacyjne obrazu i dźwięku

- Panel sterowania posiada wbudowaną regulację głośności i jaskrawości. Ponieważ każdy panel sterowania jest regulowany indywidualnie, zmiana głośności czy jaskrawości w jednym z nich nie ma wpływu na inne panele w tym samym systemie.

Różne Języki

- Dla każdego nowo utworzonego użytkownika wybiera się preferowany język (angielski, niemiecki, francuski i holenderski). Po zalogowaniu użytkownika w panelu sterowania ustawiany jest preferowany język.

Wejście tampera

- Obudowa panelu sterowania posiada wbudowany tamper wykrywający oderwanie od ściany lub zdjęcie pokrywy.

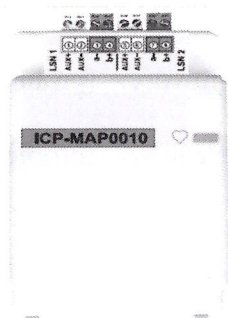
Parametry mechaniczne

- Wymiary: 146x171,5x44,5 mm
- Masa: 600 g
- Właściwości ekranu dotykowego: panel TFT-LCD o przekątnej 14 cm (5,7"); 320 x 240 pikseli z 16-bitową paletą barw; białe diody LED podświetlenia z regulowaną jasnością (podświetlenie aktywne i spoczynkowe); proporcja boków = 4:3
- Materiał obudowy: biały plastik fakturowany
- Wskaźniki: trzy diody LED
 - zielona: zasilanie
 - żółta: usterka
 - czerwona: alarm
- Połączenia: 4-żyłowa magistrala BDB (dane i zasilanie); 2 zestawy zacisków do okablowania łańcuchowego wejść / wyjść; zacisk śrubowy lub przełącznik do okablowania odgałęzienia

Komunikacja pętlowa

Wewnętrzna magistrala sieciowa pracuje w oparciu o protokół CAN (ang. Controller Area Network), łącząc centralę alarmową z takimi elementami systemu jak bramy pętlowe, zasilacze, interfejsy użytkownika w postaci ekranów dotykowych oraz moduły komunikacji z portami szeregowymi i równoległymi. Ponadto technologia Can-Bus zapewnia komunikację do 1000 metrów, co pozwala na obsługę rozległych obiektów. Zewnętrzna magistrala sieciowa IP zapewnia połączenie z systemami zainstalowanymi w innych budynkach. Dzięki otwartym interfejsom istnieje możliwość integracji centrali alarmowej z innymi systemami bezpieczeństwa i automatyki budynkowej. W przypadku współpracy ze zintegrowanym systemem automatyki budynkowej systemem można sterować bezpośrednio za pomocą stacji roboczej. Obsługa oświetlenia, trasy strażników, kontrola dostępu czy obsługa systemów sygnalizacji włamania - wszystkimi tymi zadaniami można kierować z jednej lokalizacji.

Moduł bramy pętlowej



Każda z bram jest połączona z jedną pętlą lub dwoma liniami otwartymi o maksymalnym obciążeniu wyjściowym 300 mA. Każda brama obsługuje maksymalnie 127 urządzeń adresowalnych. Konfiguracja z obwodem pętli toleruje pojedynczy stan zwarcia lub otwarcia przy zapewnieniu pełnej funkcjonalności w pętli. Brama obsługuje dwa pojedyncze wyjścia nadzorowane z zabezpieczeniem przeciwprzepięciowym.

Parametry :

- Obsługuje maksymalnie 127 urządzeń, maksymalne obciążenie pętli 300 mA
- Umożliwia utworzenie elastycznych struktur sieci (jedna pętla lub dwie linie otwarte)
- Zapewnia nadmiarowość po jednej awarii w konfiguracjach z pętlą (nie w konfiguracjach z liniami otwartymi)
- Wyposażony w dwa pomocnicze wyjścia zasilania (500 mA każde)

Dane techniczne

Parametry elektryczne

- Minimalne napięcie robocze (V DC) 16
- Maksymalne napięcie robocze (V DC) 29
- Napięcie znamionowe (V DC) 28
- Natężenie znamionowe (mA) 1600

Pobór prądu w trybie gotowości

- Maksymalne natężenie prądu wyjściowego AUX (mA) 2 x 500
- 3 Moduł bramy

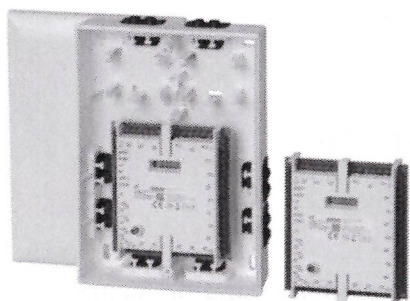
Parametry mechaniczne

- Wymiary (cm) (wys. x szer. x głęb.) 15.88 x 8.26 x 6.35
- Masa (g) 365
- Materiał obudowy
- Tworzywo ABS
- Kolor biały
- Wskaźnik Zielona dioda LED zasilania

Parametry środowiskowe

- Minimalna temperatura robocza (°C) -10
- Maksymalna temperatura robocza (°C) 55
- Minimalna temperatura magazynowania (°C) -20
- Maksymalna temperatura magazynowania (°C) 60
- Minimalna wilgotność względna (%) 5 (bez kondensacji)
- Maksymalna wilgotność względna (%) 95 (bez kondensacji)
- Klasa ochronna IP30, IP31
- Poziom zabezpieczeń IK04, IK06
- Klasa środowiskowa II: EN50130-5, VdS 2110
- Wykorzystanie wewnętrzne

Moduł wejść/ wyjść



Do dołączenia elementów konwencjonalnych wykorzystuje się moduł urządzeń konwencjonalnych. Obsługuje on 6 wejść w konfiguracji NC, EOL i DEOL, a także 4 wyjścia. Moduł instaluje się na pętli podobnie jak urządzenia detekcyjne wykonane w pętli. Element monitoruje linię główną pod kątem występowania alarmu, zwarcia i przerwy. Posiada Rozbudowane systemowe wartości graniczne w „ulepszonej wersji” trybu i oraz styk antysabotażowy (alarm antysabotażowy).

Parametry elektryczne:

Część pętlowa:

- Minimalne napięcie robocze (VDC) 15
- Maksymalne napięcie robocze (VDC) 33
- Maksymalny pobór prądu (mA) 4.95

Inne funkcje modułu rozszerzenia :

- Minimalne napięcie robocze (VDC) 9
- Maksymalne napięcie robocze (VDC) 30
- Maksymalny pobór prądu (mA) przy 12V 370
- Maksymalny pobór prądu (mA) przy 28V 180

Urządzenia zewnętrzne

- Minimalne napięcie wyjściowe (VDC) 11.9
- Maksymalne napięcie wyjściowe (VDC) 16.3

Urządzenia detekcyjne (czujki, przyciski):

Podczas projektowania systemu sygnalizacji włamania i napadu przyjęto następujące założenia:

- w oparciu o analizę zagrożeń dla obiektu system powinien być wykonany w oparciu o urządzenia, co najmniej stopnia 2 (wg PN-EN50131)
- w celu zwiększenia niezawodności działania, magistrala czujek musi mieć możliwość zamknięcia w pętli
- ochrona oparta o adresowalne czujki ruchu z antymaskingiem, czujki wstrząsowe oraz adresowalne i klasyczne czujki magnetyczne

Do ochrony wnętrza pomieszczeń należy zastosować pasywne czujki podczerwieni oraz czujki dualne. Zaleca się zastosowanie czujek wyposażonych w funkcję antymaskingu dla zapewnienia wyższego poziomu ochrony.

Minimalne parametry czujek:

- Zasięg minimum 18 x 25 m i możliwość wyboru krótkiego zasięgu co najmniej 8 x 10 m
- Technologia przetwarzania sygnałów z kilku detektorów
- Aktywna redukcja białego światła
- Dynamiczna kompensacja temperaturowa
- Wysokość montażu od 2 do 3 m; bez konieczności regulacji
- Zgodność z normą EN50131-2-4, stopień 2
- Zdalny autotest
- Zakres napięć zasilania: od 9 do 28VDC
- Praca w technologii dwuprzewodowej (współpraca z centralą opartą na technologii CAN poprzez szeregowy złącze komunikacyjne magistrali adresowej)

- Trójogniskowy układ optyczny zapewniający trzy długości ogniskowania: soczewka dalekiego, średniego i krótkiego zasięgu
- Dwa detektory piroelektryczne zapewniające wzmocnienie optyczne

Czujka typu TriTech+ z antymaskingiem

Czujki TriTech+ z funkcją antymaskingu MANTIS posiadają te same właściwości detekcyjne zarówno w wersji adresowalnej jak i konwencjonalnej. Inny jest jedynie sposób podłączenia i późniejszej konfiguracji – w ujęciu adresowalnym czujka przesyła wszystkie rodzaje alarmów, jest konfigurowana, a także zasilana poprzez połączenie 2-żyłowe bez konieczności fizycznej zmiany przełączników na urządzeniu.

Główne funkcje:

Technologia przetwarzania sygnałów z kilku detektorów (Sensor Data Fusion):

Czujka dualna powinna korzystać z algorytmu przetwarzania danych z kilku źródeł w celu zapewnienia jak najwyższej skuteczności wykrywania bez narażania inwestora na ryzyko wystąpienia fałszywego alarmu. Wbudowany mikrokontroler powinien dokonywać analizy sygnałów ze źródeł co najmniej dwóch detektorów piroelektrycznych, detektora mikrofalowego o regulowanym zasięgu, detektora temperatury i detektora poziomu białego światła, a także dedykowanego obwodu antymaskingu.

Optyka:

Układ optyczny czujki powinien wykorzystywać trzy soczewki, które zapewnią trzy różne długości ogniskowej dla dalekiego, średniego i bliskiego zasięgu wykrywania. Wspomniane długości powinny dzielić obszar na 86 stref wykrywania w celu uzyskania do 11 kurtyn detekcji. Czujka wyposażona w dwa detektory piroelektryczne powinna dodatkowo zapewnić podwójne wzmocnienie sygnału w odniesieniu do podstawowych rozwiązań stosowanych na rynku.

Antymasking (MANTIS):

Czujka powinna zapewniać funkcję wielopunktowego wykrywania maskowania. Funkcja ma chronić przed celowym lub nieumyślnym ograniczaniem zasięgu lub właściwości detekcyjnych urządzenia i wysyłać alarm nawet w przypadku, gdy strefa detekcyjna nie jest uzbrojona. Ważne jest, aby zastosowany algorytm spełniał międzynarodowe normy dotyczące wykrywania obiektów maskujących z uwzględnieniem wielu materiałów, takich jak tkaniny, papier, metal, plastik, taśmę i spray. Do detekcji wspomnianych elementów czujka powinna używać do trzech niezależnych technologii dedykowanych do danego rodzaju sposobu maskowania.

Redukcja światła białego:

Czujka powinna posiadać wbudowany detektor światła białego do pomiaru wiązki padającej nań bezpośrednio, a mogącej wywołać fałszywy alarm lub ograniczyć zdolności detekcyjne. Pomiar wiązki światła padającego powinien być wykorzystywany przez algorytm przetwarzania sygnałów z kilku detektorów, w celu dostosowania odpowiednio czułości dla wszystkich komponentów urządzenia.

Kompensacja temperatury otoczenia:

Czujka powinna posiadać funkcję pomiaru temperatury otoczenia w celu dostosowania czułości pozostałych podzespołów. Kompensacja temperatury powinna umożliwiać stałe odróżnianie potencjalnych intruzów w jak najszerszym zakresie temperatur, co jest szczególnie ważne dla zakresu temperatur zbliżonych do temperatury ludzkiego ciała.

Regulacja zasięgu:

Standardowy zasięg czujki powinien wynosić przynajmniej 18 x 25 m przy czym producent powinien dodatkowo zapewnić opcję wyboru zasięgu krótkiego, np. 8 x 10 m, który mógłby być wykorzystywany w aplikacjach o ograniczonej przestrzeni ze względu na różne czynniki organizacyjne. *(W przypadku czujki konwencjonalnej to mikroprzełącznik, a w czujkach adresowalnych zmianę zasięgu edytuje się zdalnie, za pomocą oprogramowania do konfiguracji centrali bez konieczności zdejmowania pokrywy czujki).*

Ochrona antysabotażowa:

Czujka powinna oferować możliwość monitorowania zdjęcia obudowy lub oderwania od ściany w celu detekcji zachowania sabotażowego.

Dioda LED:

Czujka powinna być wyposażona w diodę LED, która służy do wykonania poprawnego obchodu testowego. W aplikacjach pracy normalnej dioda LED nie powinna zdradzać swoim zachowaniem zasięgu wykrywania, aby nie dostarczać tego typu informacji dla potencjalnych intruzów znajdujących się w obiekcie podczas gdy system nie jest uzbrojony. Jasność diody LED powinna dostosowywać się do otoczenia automatycznie analizując wcześniej poziom światła w otoczeniu.

Pamięć alarmów i usterek:

Czujka powinna zapewniać pamięć alarmów. Pamięć alarmów powinna być sterowana zewnątrz, np. poprzez sterowanie napięciem z centrali alarmowej.

Auto test:

Czujka powinna oferować funkcję zdalnego auto testu, którą można wywołać z zewnątrz. W razie niepowodzenia testu czujka powinna uaktywnić przekaźnik odpowiedzialny za usterkę.

Odporność:

Czujka swoją budową powinna zapewniać odporność na czynniki środowiskowe minimalizując jednocześnie ryzyko spowodowania fałszywego alarmu. Czujka powinna oferować hermetycznie zamkniętą obudowę, podczas instalacji której ryzyko uszkodzenia lub zabrudzenia któregośkolwiek z elementów optycznych lub detekcyjnych będzie uniemożliwione. Zwarta budowa powinna zabezpieczać czujkę przed cyrkulacjami powietrza, pyłem i owadami, a specjalnie dostosowana czułość powinna zabezpieczać czujkę przed fałszywymi alarmami wywołanymi przez zwierzęta do 4,5 kg, np. gryzonie.

Programowanie:

Czujka powinna zapewniać czytelny dostęp do mikroprzełączników służących do programowania funkcji czujki. W przypadku wersji adresowalnej czujkę konfiguruje się zdalnie z poziomu aplikacji inżynierskiej lub z poziomu centrali alarmowej.

OPIS:

Czujka powinna zapewniać trzy aktywne technologie detekcji zamaskowania. W tym celu urządzenie powinno używać czterech aktywnych emiterów podczerwieni i trzech fotodiod. Zastosowanie powyższych podzespołów powinno służyć detekcji czynników maskujących, a zatem ograniczać ryzyko umyślnego i nieumyślnego upośledzania zdolności detekcyjnych urządzenia.

Opis poszczególnych technologii:

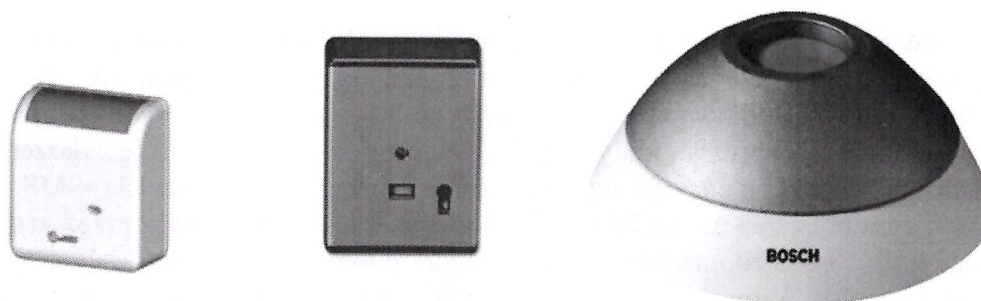
Pierwsza z aktywnych technologii (Bounce back technology) używanych do wykrywania maskowania powinna zapewniać ochronę przed przedmiotami ograniczającymi zasięg urządzenia

bezystykowo, jak na przykład pudełko do butów lub po prostu elementy zwisające z sufitu. W tym celu czujka powinna emitować promieniowanie IR tworzące wokół niej sferę o promieniu 30 cm mierzonego od środka urządzenia. W momencie normalnej pracy i braku zakłóceń w wartości emitowanej wiązki przekaźnik antymaskingu jest niewykorzystywany. Alarm zostaje wyzwalany po pojawieniu się w zasięgu sfery materiału obiektu maskującego.

Druga z technologii (Retro reflector) dotyczy wykrywania próby zamalowania czujnika np. farbą w sprayu lub lakierem. Dioda czujki znajdująca się w przedniej części nie jest tylko wskaźnikiem, a jednocześnie jest strukturą złożoną z wielu pryzmatów, które służą do odbijania energii IR generowanej z wnętrza czujki. W przypadku, gdy czujka zostaje pomalowana na granicach ośrodków dochodzi do załamania fali a co za tym idzie zmienia się współczynnik odbicia uaktywniając alarm.

Trzecia technologia (Through the lens) polega na detekcji próby maskowania strefy podejścia czujki. Dwa pryzmaty umieszczone przy strefie dolnej rozpraszają promieniowanie IR, a znajdująca się dedykowana fotodiody sprawdza w sposób ciągły poziom promieniowania.

13.7. System sygnalizacji napadu stacjonarny.



Rysunek 13.6. Przykładowe elementy systemu antynapadowego / pomocy

Rozmieszczenie poszczególnych urządzeń wskazano na rysunkach technicznych w części graficznej u uwzględniając podstawowe założenia dotyczące wyposażenia w system przestrzeni biurową (sekretariat, dyrektor placówki) oraz wystawową tzn. zlokalizowane w miejscach dostępnych dla personelu oraz pracowników ochrony (miejscas dobrane pod kątem wyposażenia wystawienniczego na bazie projektu konserwatorskiego.)

W projekcie zastosowano stacjonarne, adresowane przyciski antynapadowe dedykowane do systemu w stopniu 3 według normy PN-EN 50131-3:2010 Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 3: Urządzenia sterujące i obrazujące.

Każdorazowe użycie (wciśnięcie przyciski) powodują opisaną w dziale integracji systemów reakcje na zdarzenie. Przycisk generuje alarm w formie czasowej bez konieczności resetu elementu.

Charakterystyka przycisku

- Przycisk antynapadowy w technologii pętlowej
- Do podłączenia do antywłamaniowego panelu sterowania
- Przekazywanie sygnału alarmu i sabotażu za pomocą magistrali pętlowej
- Styk antysabotażowy Kabel do montażu natynkowego lub podtynkowego
- Nakładka z pokrywą, jako zabezpieczenie przycisku (opcjonalna)

Specyfikacja techniczna

- Napięcie robocze (część pętlowa) Od +12 V do 30 V
- Zużycie prądu (napięcie liniowe) Ok. 0,5 mA
- Temperatura otoczenia Od - 0°C do +50°C
- Warunki otoczenia DIN 40040 R14
- Klasa ochrony IP 40
- Obudowa
- Materiał ABS
- Kolor RAL 9002 (obudowa)
- Szary (osłona)
- Masa ok. 70 g
- Wymiary (gł. x wys.) 81 x 31 mm
- Klasa środowiskowa 2

Przypisanie przycisku do danej strefy użycia zostanie rozwiązane w sposób organizacyjny i opisany w SSWiN i SMS w uzgodnieniu z Zamawiającym.

13.8. Bezprzewodowy system antynapadowy SN

W ramach budowy systemu sygnalizacji napadu wskazuje się na zastosowanie systemu bezprzewodowego pracującego, jako system wspomagający. Konfiguracja uwzględnia wykorzystanie urządzeń przekaźnikowych wielokanałowych, pracujących w ramach odseparowanej galwanicznie struktury (np. poprzez moduły wejść). Użycie przycisku generuje zdarzenia typu NAPAD w systemie SWiN oraz przekazuje zgodnie z koncepcją alarm na stanowisko SMS.

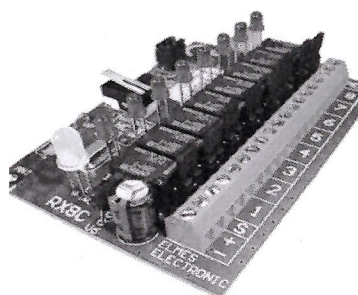
Konfiguracja systemu musi zapewniać identyfikację użycia każdego pilota poprzez zadziałanie dedykowanego przekaźnika. Każdorazowe użycie danego pilota musi aktywować dedykowaną linię/ wejście modułu EMIL. Konsekwencją rozwiązania będzie identyfikacja sygnału napadu z rozróżnieniem aktywacji poszczególnych pilotów. W tym zakresie projekt dopuszcza zastosowanie i budowę osobnego systemu antynapadowego opartego o urządzenia bezprzewodowe z rozróżnieniem poszczególnych przycisków oraz integracją z systemem SMS. Np. Zastosowanie centrali alarmowej z modułem TCP/IP (podłączona do integratora SMS, jako osobny podsystem) z podłączonymi odbiornikami przycisków bezprzewodowych. Należy zaznaczyć, że w takim wypadku wykonawca musi zapewnić podobne parametry zasilania awaryjnego zgodne z bilansem prądowym pozostałej części systemu antynapadowego opartego o przyciski stacjonarne (bilans systemu SSWiN) oraz pełne pokrycie zasięgiem pilotów w całej przestrzeni obiektu (pokrycie zasięgiem całego obiektu musi być zapewnione dla każdego z rozwiązań systemu antynapadowego).

Budowa systemu antynapadowego bezprzewodowego ma umożliwiać przekazanie sygnału użycia przycisku bezprzewodowego w całym budynku i w promieniu 10 m od zewnętrznych ścian budynku. Pozostałe elementy bezprzewodowe należy dobrać pod kątem wyposażenia pracowników patrolowych ochrony fizycznej oraz wyznaczonych pracowników obsługi przestrzeni wystawy (ilość pilotów określona na bazie uzgodnień roboczych).



Rysunek 13.7. Przykładowe elementy systemu antynapadowego / pomocy

13.8.1. Parametry systemu



Rysunek 11.8 Odbiornik 8 kanałowy. Odbiornik superheterodynowy CH8HR

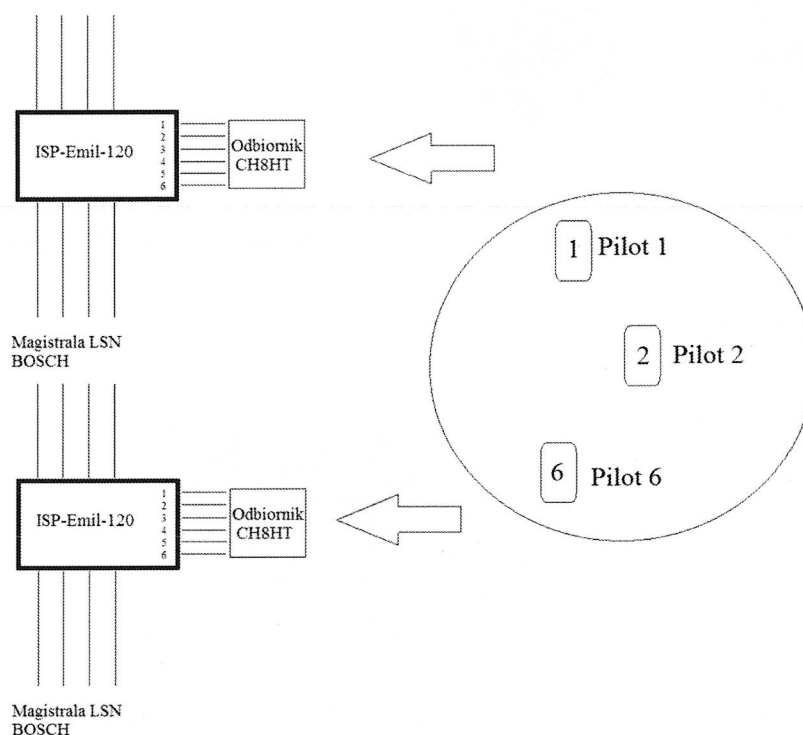
Odbiornik przeznaczony jest do bezprzewodowych systemów alarmowych i zdalnego sterowania, w których używa się wielu nadajników z dynamicznym kodem zmiennym i wymagana jest ich identyfikacja. Posiada 8 wyjść przełącznikowych typu NO (normalnie rozwarte) lub NC (normalnie zwarte) separowanych galwanicznie oraz 8 diod LED do optycznej sygnalizacji załączenia wyjść przełącznikowych. Sygnalizuje rozładowanie baterii w nadajnikach i otwarcie obudowy (antysabotażowa funkcja TAMPER) oraz brak łączności z detektorami (PTX, GBX, CTX4H). Współpracuje ze wszystkimi nadajnikami i pilotami Elmes. Do każdego kanału odbiornika można przypisać dowolną ilość nadajników, ale łączna ich ilość w systemie nie może przekroczyć 40. Piloty wielokanałowe oraz nadajnik RP501 przełączają zawsze kolejne, sąsiadujące ze sobą kanały. Detektory PTX50, GBX, CTX pracują w dwóch kanałach: detekcja w dowolnym kanale od 1 do 8, a antisabotaż w kanale 8 przydzielanym automatycznie.

Podstawowe parametry:

- częstotliwość pracy 433,92MHz, odbiornik superheterodynowy,
- współpraca ze wszystkimi nadajnikami ELMES 433,92MHz,
- maksymalna ilość nadajników 40,
- 8 wyjść przełącznikowych NO/NC, praca włącz/wyłącz lub czasowa,
- sygnalizacja załączenia kanałów na diodach LED,
- sygnalizacja słabej baterii nadajników.

Przykładowe parametry pilota antynapadowego

- częstotliwość pracy 433,92MHz;
- moc < 10mW;
- bateria 9V;
- wymiary (dł/szer/wys) 113/33/21mm.



Rysunek 11.9 przykładowy schemat podłączenia systemu antynapadowego

Zastosowanie podwójnej ochrony antynapadowej pozwoli zaspokoić wymagania stawiane obiektowi jednocześnie zapewniając właściwy stopień zabezpieczenia (system SSWiN).

13.8.2. Charakterystyka

Podsystem zorganizowany, jako autonomiczna struktura odseparowana galwanicznie od istniejącego systemu SSWiN zgodnie z dostępnymi rozwiązaniami rynkowymi. W ramach organizacji sprzętowej należy wykonać infrastrukturę opartą o urządzenia dublujące system stałych przycisków. Każdy z zastosowanych odbiorników /pilotów alarmowych musi przysyłać w trybie on-line do centrali alarmowej następujące komunikaty:

- stan spoczynku
- stan naruszenia
- stan alarmowy
- stan sabotażu
- stan bliskiego wyczerpania baterii zasilającej

13.8.3. Funkcjonalność

Funkcjonalność systemu antynapadowego opiera się w głównej mierze na doposażeniu stacjonarnego systemu antynapadowego pracującego na bazie systemu SSWiN. Element bezprzewodowy jest systemem uzupełniającym i rozszerzającym możliwości systemu poprzez wywołanie alarmu napadu z przenośnego przycisku radiowego dla:

- Pracowników WSO – patrol
- Pracowników WSO - dedykowany posterunek
- Pracownik etatowy – opiekun pomieszczenia, przewodnik etc.

W zakresie dopuszczonych rozwiązań projekt wskazuje na zastosowanie radiolinii o dużym zasięgu (z powodu znacznej grubości ścian i konstrukcji budynku) z potwierdzeniem odebrania sygnału.

Oczekiwana funkcjonalność radiolinii:

Przyciśnięcie przycisku pilota spowoduje zapalenie diody informacyjnej (zadziałania urządzenia przenośnego) i wysłania cichego powiadomienia pracownika monitoringu. Otrzymanie sygnału (odebranie przez odbiornik radiolinii) jest potwierdzone innym kolorem (np. zielony) na pilocie. Opcja znacząco podnosi pewność wezwania pomocy przez osobę wzywającą służbę WSO.

System ochrony antynapadowej (mobilnej) zostanie podłączony do aplikacji integrującej SMS. Wszystkie komunikaty alarmowe, techniczne będą zwizualizowane na mapie klienta PC w celu szybkiej oceny sytuacji przez pracownika WSO. Konfiguracja systemu umożliwi operatorowi stacji klienckiej podstawową obsługę systemu pod kątem codziennej funkcjonalności polegającej na :

- Kasowaniu alarmów napadowych bez możliwości rozbrajania wybranej strefy lub grup stref;
- Przeglądaniu historii zdarzeń;

Wywołanie zdarzenia typu alarm napadowy* powoduje rozpoczęcie algorytmu działania w następujących zależnościach:

- Alarm dźwiękowy w aplikacji SMS oraz SSWiN;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania alarmu z dokładnością do przycisku, który go wygenerował (identyfikacja zadziałania pilota bezprzewodowego);
- Określenie typu alarmu tzn.: napad;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem sposobu postępowania i listy osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne, ochrona zewnętrzna etc.

* Uwaga: wyjątek stanowi wywołanie alarmu napadowego w pomieszczeniu monitoringu. Dla tego przypadku sygnał powinien zostać wysłany do zewnętrznych służb ochronnych np. zmotoryzowanego patrolu/zespołu interwencyjnego. Do ustalenia na etapie wykonawczym.

13.9. Charakterystyka SSWiN

Wykonany system musi uwzględniać zabezpieczenia okien na poziomie piwnicy, parteru oraz w Sali Wilanowskiej planuje się wykonać w całości w II etapie inwestycji. Na pozostałych kondygnacjach w drugim etapie inwestycji należy doprowadzić do okien drożne trasy kablowe, z wprowadzonym przewodem, od głównych tras kablowych, od strony okien zakończone puszką podtynkową z sygnalizacją otwarcia. Zapas przewodu umożliwiający późniejsze podłączenie czujników pozostawić po stronie głównych tras kablowych.

System alarmowy zorganizowany jest, jako struktura pętlowa – magistralowa z pełną adresacją elementów detekcyjnych – czujek alarmowych i przycisków do sygnalizacji napadu.

Każdy z zastosowanych elementów detekcyjnych przesyła do centrali alarmowej komunikaty zgodnie z 2 stopniem zabezpieczenia oraz dodatkowo stan zasłonięcia czujki ruchu (zamaskowania) oraz zapewnia regulację podstawowych parametrów pracy bezpośrednio z aplikacji zarządzającej centralą alarmową. Funkcja ta jest stosowana dla obsługi urządzeń zlokalizowanych w trudno dostępnych miejscach, uniemożliwiających regulację urządzeń bez ingerencji (przesuwanie,

zdejmowanie etc.) w eksponaty wystawowe lub inne wyposażenie muzealne tj. demontaż gablot, osłon, zabezpieczeń mechanicznych.

Dla czujki otwarcia stykowej (zewnętrznej) chroniącej strefę (właz studzienki kablowej) rewizji teletechnicznej zastosowano separację galwaniczną od SSWiN.

13.10. Funkcjonalność SSWiN

System sygnalizacji włamania i napadu zostanie podłączony do aplikacji integrującej SMS. Wszystkie komunikaty alarmowe i techniczne generowane przez SSWiN będą zwizualizowane na mapie synoptycznej stacji roboczej stanowiska operatorskiego (klienta PC). Konfiguracja systemu umożliwi zarówno użytkownikowi (klawiatury LCD) jak i operatorowi SMS pełną obsługę systemu pod kątem codziennej funkcjonalności polegającej na :

- Uzbrajaniu / rozbijaniu poszczególnych stref alarmowych z uwzględnieniem uprawnień poszczególnych kodów;
- Kasowaniu alarmów bez możliwości rozbijania wybranej strefy lub grup stref;
- Blokowaniu / odblokowaniu poszczególnych stref alarmowych, detektorów z uwzględnieniem hierarchizacji uprawnień;
- Aktywacji zaprogramowanych funkcji korelacji międzysystemowych np. aktywacja i dezaktywacja automatyki otwarcia drzwi wejściowych dla gości z pozycji centrali oraz aplikacji SMS;
- Przeglądaniu historii zdarzeń.

SSWiN musi zapewnić hierarchiczność kodów dostępu i skalowalność stref alarmowych. Wymaga się, aby system umożliwiał utworzenie minimum 50 stref alarmowych.

W podstawowym zakresie proponuje się skonfigurowanie 30 stref dostępu tzn.:

- Strefa korytarzowa 1 poziom piwnicy – korytarze komunikacyjne, toalety etc.;
- Strefa korytarzowa 2, 3 poziom od 0 do +1 – korytarze komunikacyjne, toalety etc.;
- Strefa korytarzowa 4 poziom od 2 – korytarze komunikacyjne, toalety etc.;
- Strefa zewnętrzna 5 poziom +1 – balkony zewnętrzne ;
- Strefa wystawiennicza 5 do 15 – poziomy 0 do +2;
- Strefa gastronomiczna 16,17 – część zaplecza poziom parteru oraz poziom piętra +1;
- Strefy magazynowa 18-25 dla poszczególnych pomieszczeń magazynowych;
- Strefy biurowe 25,26,27 dla poszczególnych poziomów;
- Strefa dyrekcji 28,29 – sekretariat, dyrektor;
- Strefa magazynu WSO 30- magazyn broni;
- Strefa serwerowa 31 – serwerownia.

Zastosowany SMS oraz jego konfiguracja mają zapewnić monitorowanie wszystkich sygnałów generowanych przez SSWiN. Integracja SSWiN z SMS musi uwzględniać programowe połączenie funkcjonalne pozostałych systemów i ich reakcję na otrzymany z systemu sygnał.

Dla przykładu:

Wywołanie zdarzenia „**alarm włamaniowy**” powoduje następującą sekwencję reakcji/zadziałań:

- Alarm dźwiękowy w klawiaturach LCD;
- Alarm dźwiękowy w przyporządkowanych do stref sygnalizatorach optyczno-akustycznych;
- Alarm dźwiękowy w aplikacji SMS;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania alarmu z dokładnością do pomieszczenia i czujnika, który go wygenerował;

- Wyświetlenie na monitorze systemu SMS obrazu z kamery obserwującej strefę w alarmie lub jej najbliższą z możliwością zaprogramowania czasu wyprzedzenia, z jakim ma się wyświetlać obraz z nagrania;
- W przypadku alarmu z pomieszczeń graniczących z zewnętrznymi ścianami skierowanie kamery PTZ na strefę w stanie alarmu;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem postępowania i parametrów osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne etc;

Wywołanie zdarzenia „alarm napadowy”^{*)} powoduje następującą sekwencję reakcji/zadziałań:

- Alarm dźwiękowy w aplikacji SMS;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania alarmu z dokładnością do pomieszczenia i przycisku, który go wygenerował;
- Określenie typu alarmu tzn.: napad, sabotaż, jako równoważne zdarzenie z sygnałem napadu;
- Wyświetlenie na monitorze systemu SMS kamery obserwującej strefę w alarmie lub jej najbliższą z możliwością zaprogramowania czasu wyprzedzenia, z jakim ma się wyświetlać obraz z nagrania;
- W przypadku alarmu z pomieszczeń graniczących z zewnętrznymi ścianami skierowanie kamery PTZ na strefę w stanie alarmu;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem postępowania i parametrów osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne, ochrona zewnętrzna etc.

^{*)} **Uwaga:** wyjątek stanowi wywołanie alarmu napadowego z pomieszczenia monitoringu. Dla tego przypadku sygnał powinien zostać wysłany do zewnętrznych służb ochronnych (stacji monitoringu alarmów) i spowodować wysłanie zmotoryzowanego patrolu (grupy interwencyjnej). Do ustalenia na etapie wykonawczym.

Sygnalizacja typów sygnałów alarmowych i technicznych generowanych przez SSWiN zostanie ustalona z Zamawiającym na etapie wykonawczym.

13.11. Zasilanie SSWiN.

System SSWiN jest zasilany z dwóch źródeł: podstawowego i rezerwowego. Zasilanie podstawowe jest realizowane z sieci elektroenergetycznej 230V/50Hz. Natomiast zasilanie rezerwowe jest oparte na baterii akumulatorów z zasilaczem buforowym typu A. Pojemność baterii akumulatorów wynika z bilansu mocy z czasem gotowości odpowiednim dla 2. stopnia zabezpieczeń. Ze względu na zastosowanie alternatywnego zasilania podstawowego – agregatu prądotwórczego włączanego po zaniku zasilania podstawowego – czas gotowości rezerwowego zasilacza **typu A** wynosi **24 godziny**. Rezerwowe źródło zasilania jest doładowywane do 80% pojemności w czasie nie dłuższym niż **72 godziny**.

Tabela 13-1. Szacunkowy bilans mocy systemu SSWiN

Lp.	Rodzaj	Typ	Ilość	Prąd spoczynkowy Ic (a)	Prąd alarmu Ia (A)	Całkowity prąd spoczynkowy Ics (A)	Całkowity prąd alarmu Ica (A)
1	Centrala alarmowa	Adresowalna	1	0,3	0,6	0,3	0,6
2	Expander rozszerzeń	Linii	6	0,06	0,12	0,36	0,72
3	Expander rozszerzeń	Wyjść	4	0,005	0,16	0,02	0,64
4	Klawiatura strefowa	Lcd	15	0,06	0,175	0,9	2,625
5	Sygnalizator wewnętrzny	Opt.-akustyczny	1	0	0,9	0	0,9
6	Czujka ruchu	PIR	28	0,005	0,005	0,14	0,14
7	Czujka ruchu	PIR/MW	96	0,005	0,005	0,48	0,48
8	Czujka ruchu	PIR - kurtyna	10	0,005	0,005	0,05	0,05
9	Czujka ruchu zewnętrzna	PIR/MW	4	0,02	0,02	0,08	0,08
10	Czujka kontaktronowa	Drzwiowa	194	0,005	0,005	0,97	0,97
		Wpuszczana					
		Nawierzchniowa					
11	Czujka inercyjna	Inercyjna	6	0,0025	0,0025	0,015	0,015
12	Przycisk antynapadowy	Adresowalny	10	0,0005	0,0005	0,005	0,005
13	Odbiornik radiowy	Bezprzewodowy	2	0,02	0,015	0,04	0,03
14	Prąd całkowity					3,36	7,255
15	Czas pracy spoczynkowej	Ts- 24 h	Zgodnie ze wzorem $((Ts * Ics) + (Ta * Ica)) / 0,7 =$				
16	Czas pracy alarmowej	Ta- 0,25 h (15 minut)					
17	Wielkość akumulatorów $= ((24 * 3,36) + (0,25 * 7,255)) / 0,7 = 80,64 + 1,81 / 0,7 = 82,45 / 0,7 = 118 \text{ Ah}$						

Szacowana pojemność baterii akumulatorów ok. 118 Ah. Wykonawca zobowiązany jest do opracowania bilansu energetycznego SSWiN i dopasowania pojemności akumulatorów do przyjętego czasu podtrzymania i zastosowanych w trakcie realizacji urządzeń.

14.SYSTEM OCHRONY INDYWIDUALNEJ ZBIORÓW – SYSTEM BEZPRZEWODOWY (RADIOWY).

System indywidualnej ochrony zbiorów przeznaczony jest do indywidualnej ochrony eksponatów umieszczonych w gablotach oraz do zabezpieczenia innych eksponatów podczas wystaw czasowych lub stałych. W skład systemu wchodzi odbiorniki, czujki bezprzewodowe, elementy wyposażenia oraz system wizualizacji zdarzeń za pomocą mapy ochronionego obszaru z wrysowanymi w plan urządzeniami detekcyjnymi i pomiarowymi. Program do obsługi systemu jest niezależną aplikacją zainstalowaną na osobnym stanowisku komputerowym np. laptop.

Organizacja systemu alarmowego zapewnia identyfikację alarmu napadowego z dokładnością do poszczególnych rejonów pracy. Na etapie wykonawczym przewiduje się ułożenie magistrali

komunikacyjnej typu RS485 pod kontem przyszłościowej budowy dodatkowego elementu ochrony indywidualnej muzealiów. Zakres projektu wykonawczego wskazuje ułożenie w trasach komunikacyjnych dodatkowej magistrali komunikacyjnej do wskazanego systemu.

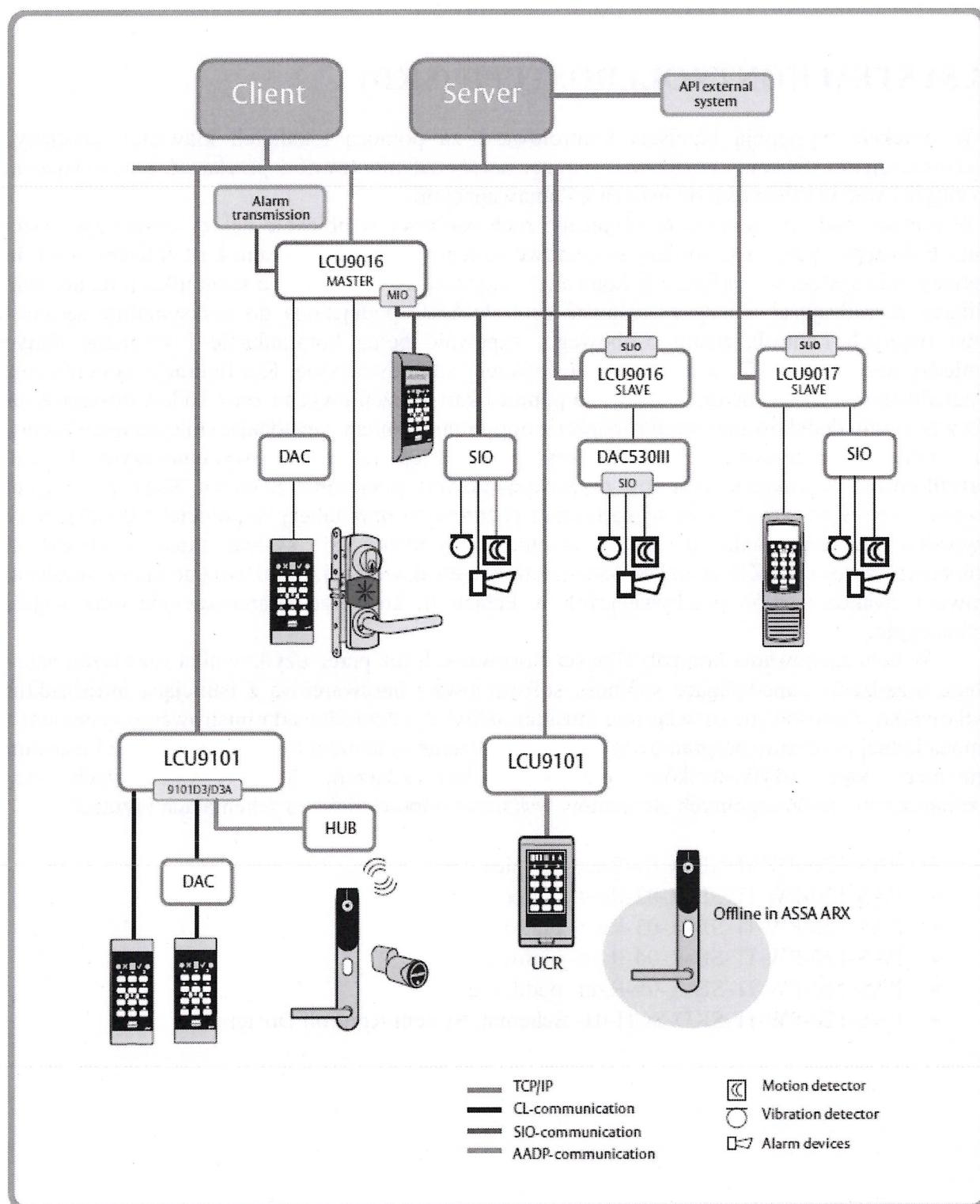
15. SYSTEM KONTROLI DOSTĘPU (SKD)

W obiekcie występują przejścia kontrolowane za pomocą lokalnych klawiatur sterujących elektrozaczepami. Obecnie użytkowany sprzęt należy zdemontować i przekazać Zamawiającemu lub zutylizować w zależności od ustaleń z Zamawiającym.

W ramach budowy systemu regulującego ruch osobowy w obiekcie należy dostarczyć system kontroli dostępu oparty o kontrolery systemowe zintegrowane z czytnikami kart zbliżeniowych lub alternatywnie system w konfiguracji kontroler – czytnik. Do zapewnienia komunikacji na poziomie aplikacji zarządzającej należy zastosować centralę SKD podłączoną do maksymalnie szesnastu drzwi objętych kontrolą ruchu osobowego, zapewnić pełną komunikację i wymianę danych pomiędzy serwerem SKD, a dedykowaną aplikacją administracyjną. Konfiguracja systemu musi uwzględniać możliwość otwarcia drzwi za pomocą kart zbliżeniowych (oraz kodów dostępowych) oraz z poziomu dedykowanej stacji roboczej z oprogramowaniem zarządzającym systemem kontroli oraz aplikacji integrującej SMS. Należy przewidzieć na etapie wykonawczym fizyczne (certyfikowane w zakresie ochrony przeciwpożarowej) połączenie systemu SKD z systemem przeciwpożarowym. Zgodnie ze scenariuszem pożarowym oraz tabelą współdziałania urządzeń w przypadku wygenerowania alarmu II stopnia z systemu SSP system musi automatycznie odblokować przejścia SKD zlokalizowane na drodze ewakuacyjnej, umożliwiając przeprowadzenie sprawnej ewakuacji osób przebywających w Pałacu tj. korytarze komunikacyjne oraz wyjścia ewakuacyjne.

W celu zachowania kompatybilności stosowanych już przez użytkownika rozwiązań należy dobrać urządzenia zapewniające spójność softwareową i hardwareową z istniejącą infrastrukturą użytkownika. Zastosowane rozwiązanie musi umożliwiać jednorodne administrowanie systemem za pomocą jednej platformy programowej (pełne zarządzanie systemem SKD tj. dodawanie i usuwanie uprawnień, kart, użytkowników, odczyt pamięci zdarzeń, logów systemowych etc.). Rozmieszczenie poszczególnych elementów wskazano odpowiednio na schematach i rzutach:

- PAS-120-PW-IT-SB-R-01-Rzut- piwnica
- PAS-120-PW-IT-SB-R-02-Rzut- parter
- PAS-120-PW-IT-SB-R-03-Rzut- piętro 1
- PAS-120-PW-IT-SB-R-04-Rzut- piętro 2
- PAS-120-PW-IT-SB-R-05-Rzut- poddasze
- PAS-120-PW-IT-SKD-SCH-01- Schemat, System Kontroli Dostępu



Rysunek 15.1. Przykładowe schematy infrastruktury kontroli dostępu

Podstawowym elementem weryfikującym uprawnienia do przejścia są czytniki kart zbliżeniowych zintegrowane z kontrolerami systemowymi (sterownik). Wyposażenie systemu w

centralę pozwoli na scentralizowanie infrastruktury umożliwiając podłączenie do aplikacji SMS. Administrowanie kartami dostępu leży po stronie Zamawiającego. Budowa i konfiguracja SKD umożliwi administrowanie kontrolą dostępu z pom. 2.11 – monitoringu. Wykonawca utworzy konta operatorów i administratorów systemu. Poziomy dostępu do poszczególnych funkcji zostaną określone w uzgodnieniu z Zamawiającym. Zamknięcia elektromechaniczne drzwi wykorzystywane w SKD należy dobrać pod kątem typu drzwi oraz funkcjonalności przypisanych do danego przejścia (ewakuacyjne, p. poż itp.).

15.1. Zasilanie SKD

System SKD jest zasilany z dwóch źródeł: podstawowego i rezerwowego. Zasilanie podstawowe, jako zasilania sieciowe 230V/50Hz oraz dodatkowy pakiet zasilania awaryjnego wykorzystujący baterie akumulatorów.

Dla systemu SKD zostaną przewidziane osobne obwody zasilające 230V/50Hz określone w projekcie elektrycznym. Każdy z nich będzie zabezpieczony pod kątem przeciwzwarciovym oraz przeciwporażeniowym. W ramach projektu systemu zabezpieczeń wskazuje się podłączenie systemu do dedykowanego obwodu odpowiednim przewodem zasilającym tor zasilania podstawowego.

15.2. Charakterystyka

Oczekiwane właściwości kontroli dostępu muszą uwzględniać:

- obsługę czytników z wbudowaną klawiaturą numeryczną używaną, jeśli wymagany jest dostęp za pomocą karty i kodu PIN typu Mifare 13,56MHz, sektorowo kodowane;
- obsługi włączenia lub wyłączenia w dozór poszczególnych stref alarmowych SSWiN przy użyciu czytników kontroli dostępu za pomocą karty oraz kodu PIN;
- utrzymanie normalnego działania pozostałych kontrolerów w przypadku awarii dowolnego kontrolera w systemie;
- przesyłania podstawowych komunikatów alarmowych i technicznych do systemu SSWiN w przypadku awarii integratora np.: usterka, sabotaż, wejście siłowe
- pełnego alarmowania w stanie normalnej pracy o:
 - Nieuprawnionym otwarciu drzwi kontrolowanych,
 - Zbyt długim otwarciu drzwi,
 - Utracie komunikacji z dowolnym sterownikiem,
 - Użyciu karty bez uprawnień,
 - Użyciu karty nieznanej,
 - Podaniu błędnego kodu PIN (w przypadku czytników kart z klawiaturami numerycznymi),
 - Sabotażu sterownika.

Za pomocą SMS możemy co najmniej :

- Odczytywać stany online systemu – alarmy, usterki, stany informacyjne;
- Odczytywać i analizować zdarzenia archiwalne;
- Sterować (blokować, odblokować , wyłączać) poszczególne przejścia SKD;
- Przydzielać , kasować, zmieniać oraz weryfikować uprawnienia kart;
- Prowadzić aktywną obsługę w zakresie konserwacji i modyfikacji parametrów systemu.

W przypadku zastosowania przejść kontroli dostępu dwustronnych (np. pomieszczenie ochrony, wyjście techniczne etc.) należy infrastrukturę SKD wyposażać zgodnie z wymogami przeciwpożarowymi w ręczne, dwuobwodowe przyciski zwalniania blokady mechanicznej typu „wciśnij szybkę” zainstalowane od strony wewnętrznej strefy. Ich użycie wywołuje sygnał

alarmowy w SSWiN oraz stan alarmowy w aplikacji nadzorującej (SMS) oraz powoduje otwarcie obwodu zwalniającego blokadę przejścia (drzwi).



Rysunek 15.2. Przykładowy przycisk ewakuacyjny

15.3. Strefy /drzwi objęte systemem KD:

Zgodnie z poczynionymi w toku uzgodnień ustaleniami oraz funkcjonalnością użytkową Pałacu Krasieńskich należy system zaprojektować mając na względzie fizyczne odseparowanie części administracyjnej i technicznej obiektu od ruchu osobowego gości i zwiedzających. W takim przypadku należy utworzyć podstawowe strefy dostępowe tj.:

- Strefa biurowa i administracyjna – dostęp do pomieszczeń biurowych oraz wejście zewnętrzne techniczne;
- Strefa monitoringu – pomieszczenie ochrony (poziom +2);
- Strefa techniczna – pomieszczenia elektryczne, windy;
- Strefa rekreacyjno-kulturalna - zaplecze monitoringu (poziom + 2);
- Strefa wystawiennicza – strefa ogólnodostępna bez systemu SKD (automatyczne otwieranie drzwi wejściowych dla gości);

W związku z powyższym wyznacza się profile użytkowników:

- Pracownik dyrekcja (pomieszczenie dyrekcji)
- Pracownik etatowy (pomieszczenia sekretariatu, biurowe)
- Pracownik WSO (część biurowa + strefa monitoringu)
- Pracownik techniczny (część techniczna, dedykowane magazyny)
- Pracownik zewnętrzny (wejście do części kuchennej i magazynu kuchni)

Do wskazanych stref będą przydzielane uprawnienia dostępu poszczególnym grupom użytkowników:

- Osoby będące pracownikami etatowymi i czasowymi pełniącymi obowiązki wynikające z profilu i formy zatrudnienia.
- Osoby będące pracownikami firm zewnętrznych oraz własnym personelem technicznym pełniącym obowiązki w zakresie obsługi infrastruktury i wyposażenia obiektu (np. Służba ochrony);
- Osoby będące pracownikami firm zewnętrznych lub własnych będących obsadą całodobową sklepu i restauracji.

W celu realizacji powyższych funkcjonalności należy przewidzieć kontrolowanie ruchu osobowego w następujących pomieszczeniach/strefach:

Poziom -1

Drzwi prowadzące do stref technicznych i magazynowych - jednostronnie kontrolowane, pracujące w trybie 24h. Wyjście ze strefy / pomieszczenia następuje przy użyciu klamki drzwiowej z zamkiem, którego stan jest kontrolowany przez system SKD. System SKD musi kontrolować stan zamknięcia drzwi (czujka kontaktronowa) oraz zaryglowania (mechanicznego przez przekręcenie klucza).

Poziom 0

Drzwi zewnętrzne i wewnętrzne prowadzące do pomieszczeń 0.27a i 0.27b w trybie pracy 24 godziny na dobę. Przejścia do strefy zostaną objęta dwustronną (0.27b) oraz jednostronną (0.27a) kontrolą SKD. Wyjście ze strefy / pomieszczenia 0.27a następuje przy użyciu klamki drzwiowej z zamkiem, którego stan jest kontrolowany przez system SKD. System SKD musi kontrolować stan zamknięcia drzwi (czujka kontaktronowa) oraz zaryglowania (mechanicznego przez przekręcenie klucza).

Poziom +1

Drzwi prowadzące do strefy administracyjnej w trybie 24 godziny na dobę. Drzwi prowadzące do pomieszczenia 1.29 (użytkowa funkcjonalność i rejestrowanie ruchu pracowniczego). Wyjście ze strefy - pomieszczenia następuje przy użyciu klamki dedykowanej wkładki drzwiowej podłączonej do systemu. Konfiguracja klamki musi uwzględniać monitorowanie stanów zamknięcia drzwi (kontaktron) oraz przekręcenia klucza.

Poziom +2

Skrzydło południowe

Drzwi prowadzące do strefy monitoringu (pomieszczenia ochrony). Przejście w trybie 24 godziny na dobę, dwustronne. Wyjście ze strefy - pomieszczenia następuje przy użyciu karty. Drzwi do pomieszczeń administracyjnych w zakresie wejścia w strefę biurową bezpośrednio z przestrzeni klatki schodowej. Użycie przycisku ewakuacyjnego poprzez zabicie szybki zwalnia blokadę drzwiową jednocześnie przesyłając stan alarmowy do SMS i SSWiN.

Skrzydło północne

Należy przewidzieć kontrolę dostępu dla wszystkich przejść pomiędzy strefami administracyjną a wystawienniczą.

W projekcie wskazano, jako automatyczne otwarcie ewakuacyjne tylko przejścia znajdujące się na drodze ewakuacyjnej zgodnie ze scenariuszem pożarowym. W innym przypadku realizacja powyższej funkcji odbywa się za pomocą ręcznego zwolnienia blokady od wewnętrznej strony strefy w celu wyjścia awaryjnego.

W zakresie blokady SKD zastosowanej na drzwiach służbowych (drzwi zewnętrzne wschodnie) należy skonfigurować i dostosować elektro-blokadę typu motor lock w zakresie pracy jako :

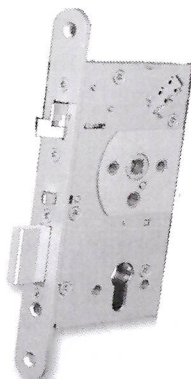
- przejście kontrolowane przez SKD
- automatyczne zwolnienie blokady SKD w przypadku alarmu z systemu oddymiania na potrzeby użycia drzwi napowietrzających. Zgodnie ze scenariuszem PPOŻ w momencie aktywacji alarmu oddymiania i uruchomienia automatyki napowietrzającej obiekt, blokada mechaniczna wykorzystywana w systemie kontroli dostępu musi umożliwić pełne otwarcie skrzydeł drzwi.

Szczegółowa konfiguracja SKD w zakresie stref dostępu zostanie uzgodniona z Zamawiającym w trakcie realizacji inwestycji.

15.4. Ogólna charakterystyka elektroblokady drzwiowej

W celu dostosowania drzwi pod kątem wyposażenia w system KD należy je wyposażać w elektrozamki typu DIN. Zastosowane rozwiązanie ma zapewnić pełną integralność i funkcjonalność z systemem SMS oraz umożliwić dostarczenie podstawowych informacji o stanie danego przejścia. W celu realizacji powyższego elektrozamek musi posiadać:

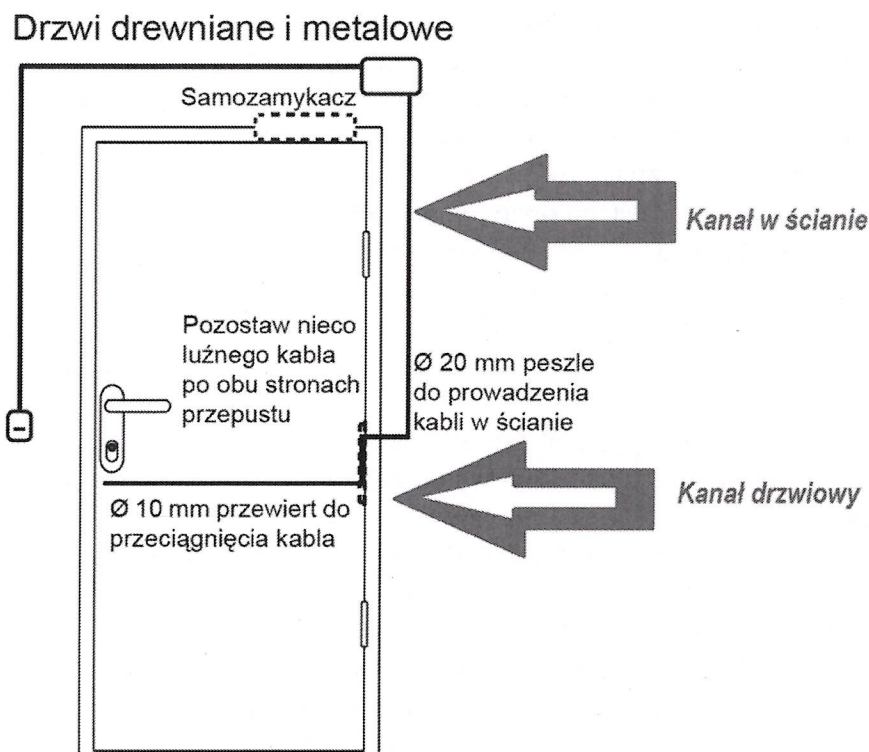
- Elektroniczny układ zapewniający zablokowanie i odblokowanie mechanizmu zewnętrznej klamki (reglamentowany dostęp z zewnątrz strefy);
- Układ styków pozwalający na wygenerowanie alarmu dla zdarzenia „wejście siłowe” (zewnętrzne otwarcie drzwi bez użycia aktywnej karty zbliżeniowej lub kodu oraz alarmowe wyjście ze strefy przy pomocy wewnętrznej klamki);
- Układ styków pozwalający na wygenerowanie alarmu dla zdarzenia „alarm sabotażowy” wewnętrznej części wkładki drzwiowej;
- Zespół styków monitorujący stan drzwi tj: otwarcie, zamknięcie, zwolnienie blokady, użycie klamki, użycie klucza etc.)



Rysunek 15.5. Przykładowa wkładka typu DIN

W celu montażu elektro blokady należy na etapie wymiany stolarki drzwiowej przygotować zespół kanałów technologicznych, niezbędnych do przeprowadzenia instalacji przewodowej sterującej wkładką elektryczną oraz pozostawić drożne trasy kablowe ściennie np. mikro kanalizację teletechniczną.

Zamek musi mieć możliwość zamocowania wkładki kluczowej. Wykonawca zamontuje wkładki kluczowe w systemie Klucza Głównego zgodnie z opisem w projekcie architektury i w uzgodnieniu z Zamawiającym.



Rysunek 15.6. Przykładowy kanał teletechniczny drzwiowy

W zakresie osprzętu stolarki drzwiowej wskazuje się konieczność wyposażenia każdego przejścia SKD w samozamykacz drzwiowy. Element należy dobrać w zależności od wielkości skrzydła, jego wagi oraz rozmiarów ościeżnicy drzwiowej zapewniając niezbędną wysokość „światła” przejścia.

15.5. Funkcjonalność

System SKD zostanie podłączony do aplikacji integrującej typu SMS oraz SSWiN. Wszystkie komunikaty alarmowe i techniczne będą zwizualizowane na mapie klienta PC w celu szybkiej oceny zdarzenia prowadzonej przez personel stanowiska monitoringu. Konfiguracja systemu musi zapewnić użytkownikowi systemu z użyciem czytników SKD:

- Przyznania na żądanie dostępu do poszczególnych stref KD z uwzględnieniem uprawnień poszczególnych kodów;
- Przyznania na żądanie dostępu do poszczególnych stref KD przez operatora stacji klienckiej, pełną obsługę systemu pod kątem codziennej funkcjonalności polegającej na:
 - Przyznania trwałego dostępu do poszczególnych stref;
 - Przyznania trwałego blokowania wybranego przejścia;
 - Odczytu historii zdarzeń
 - Administrowania systemem (opcjonalnie SMS lub dedykowaną aplikacją)
 - Aktywacji zaprogramowanych indywidualnie integracji np. blokada wybranych grupowych stref dostępu etc.

System musi zapewnić dowolną konfigurację uprawnień kart. Dla prawidłowej pracy wymaga się do utworzenia minimum 35 stref dostępowych (w przypadku potrzeby podziału stref na poszczególne pomieszczenia).

Wykonawca skonfiguruje w SKD profile operatorów oraz administratorów systemu po uzgodnieniu z Zamawiającym poziomów ich uprawnień.

Integracja systemu kontroli dostępu z systemem SMS musi uwzględniać programową interakcję funkcjonalną z pozostałymi systemami i ich reakcję na otrzymany z systemu sygnał. Wywołanie zdarzenia typu alarm – (siłowe otwarcie drzwi, sabotaż drzwi, sabotaż systemu etc.) powoduje rozpoczęcie algorytmu działania w następujących zależnościach:

- Opcjonalny alarm dźwiękowy w czytnikach SKD;
- Alarm dźwiękowy na stacji operatorskiej SMS;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania alarmu z dokładnością do pomieszczenia i czytnika, który go wygenerował.;
- Określenie typu alarmu np. sygnał wejście siłowe z czytnika „Magazyn ...”;
- Wyświetlenie na monitorze systemu STD kamery obserwującej strefę w alarmie lub najbliższą;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem sposobu postępowania i listy osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne etc;

Wywołanie zdarzenia typu Użycie karty nieznanej lub bez uprawnień powoduje rozpoczęcie logiki działania w następujących zależnościach:

- Opcjonalny alarm dźwiękowy w czytnikach SKD;
- Alarm dźwiękowy na stanowisku operatorskim SMS;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania alarmu z dokładnością do pomieszczenia i czytnika, który go wygenerował.;
- Określenie typu alarmu tzn.: sygnał wejście siłowe z czytnika „Magazyn ...”;
- Wyświetlenie na monitorze systemu STD kamery obserwującej strefę w alarmie lub najbliższą;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem sposobu postępowania i listy osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne etc;

Wywołanie zdarzenia typu technicznego (otwarcie drzwi klamką, otwarcie drzwi kluczem, otwarcie drzwi sterowaniem II stopnia z systemu SSP etc.) powoduje rozpoczęcie algorytmu działania w następujących zależnościach:

- Alarm dźwiękowy w aplikacji SMS (opcjonalnie dla zdarzeń anormalnych np. – otwarcie kluczem);
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania zdarzenia z dokładnością do pomieszczenia i elementu, który go wygenerował (otwarcie drzwi – wewnętrzna klamka);
- Określenie w systemie SMS typu zdarzenia tzn.: usterka czytnika nr..., brak zasilania 230 V etc.;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem sposobu postępowania i listy osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne oraz reakcję na zdarzenie typu „wyślij patrol...” etc;

Wywołanie zdarzenia z systemu alarmowego (alarm napadowy, alarm włamaniowy, alarm sabotażowy etc.) powoduje rozpoczęcie interakcji z systemem SKD w następujących zależnościach:

- Alarm dźwiękowy w aplikacji SMS ;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania interakcji SKD na otrzymane zdarzenie z dokładnością do pomieszczenia i elementu, który go wygenerował (np. kolor czerwony – czytnik w stanie zaryglowania przejścia spowodowanego alarmem antywłamaniowym);

- Określenie w systemie SMS typu zdarzenia np. auto zaryglowanie drzwi – alarmowe etc.;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem postępowania i parametrów osób do powiadomienia.

Uwaga: wykonawca musi zapewnić pełną zgodność systemu z zastosowanym stopniem systemu a co za tym idzie zagwarantować dostarczenie sygnałów zgodnie z wymaganiami normy PN-EN 50133-1.

Lp.	Typ	Ilość	Prąd spoczynkowy Ic (A)	Prąd alarmu Ia(A)	Całkowity prąd spoczynkowy Ica(A)	Całkowity prąd alarmu Ica(A)
1	Centrala sterująca 16 drzwi	2	0,05	0,06	0,1	0,12
2	Centrala sterująca 4 drzwi	1	0,17	0,22	0,17	0,22
3	Czytnik z kontrolerem	35	0,15	0,22	5,25	7,7
4	Blokada typu DIN	35	0,24	0,5	8,4	17,5
5	Prąd całkowity				13,92	25,54
6	Czas pracy spoczynkowej	TS =1 h				
7	Czas pracy alarmowej	TS=0,25 h - 15 minut				
8	Wielkość akumulatorów	$((TS*ICS)+(Ta*ICA)) / 0,7 =$				29 Ah

Tabela 15-1. Bilans energetyczny SKD

Szacunkowy pojemność baterii akumulatorów dla przedstawionej konfiguracji wynosi ok. 2 x 17 Ah. Wykonawca zobowiązany jest do opracowania bilansu energetycznego SKD i dopasowania pojemności akumulatorów do przyjętego czasu podtrzymania i zastosowanych w trakcie realizacji urządzeń.

16. SYSTEM ZLICZANIA OSÓB

Projektuję się system, który pozwala na analizowanie przepływu ruchu osób w Pałacu Kasińskich. Dostarcza on dane niezbędne w procesie kontroli procesów sprzedaży, jak również weryfikacji działań marketingowych.

System składa się z centrali, czujników oraz odpowiednio dobranego oprogramowania. Konfiguracja urządzeń pozwala na uzyskiwanie oczekiwanych danych.

Czujniki działające na zasadzie bariery podczerwieni powinny być zainstalowane nad wejściem. Urządzenia pomiarowe powinny posiadać możliwość oprogramowania pozwalającego na przetwarzanie i analizę zebranych danych.

17. SYSTEM WIDEOFONOWY

17.1. Stan istniejący

O obecnym stanie obiekt posiada funkcjonujący system komunikacji wideo głosowej oparty o produkt marki Bpt. Infrastruktura posiada możliwość rozbudowy o kolejne elementy wykonawcze typu kaset zewnętrzna z kamera oraz opcjonalne panele odbiorcze typu unifon z monitorem LCD. W ramach projektu należy rozbudować system o dodatkowe przejścia zachowując dotychczasową charakterystykę konfiguracji.

17.2. Rozbudowa systemu

Należy zaprojektować i doposażyć istniejący system wideo domofonowy w dodatkowy punkt nadawczo odbiorczy zlokalizowany w przestrzeni gastronomicznej pomieszczenie nr. 027c oraz dwie kasety zewnętrzne zainstalowane bezpośrednio przed drzwiami zewnętrznymi północnymi oraz odpowiednio strefy kawiarni (strefa dostawy). Dodatkowo w celu rekonfiguracji istniejące infrastruktury wideo domofonowej należy przenieść panel rozmówny (*stacja bazowa) do pomieszczenia ochrony pom. 2.11. Rozmieszczenie poszczególnych elementów systemu (kasety zewnętrzne oraz unifon z monitorem) przedstawia rysunek techniczny. Celem zadania jest rozbudowa infrastruktury bazującej na rozwiązaniu systemowym marki Bpt lub innym równoważnym zapewniającym pełną integralność z systemem pracującym w obiekcie. W obecnej konfiguracji wykorzystuje się zestaw pracujący w systemie X1, który wykorzystuje jedną parę skrętki nieekranowanej do zasilania oraz transmisji wizji, fonii i sterowań pomiędzy panelem wejściowym i zasilaczem a odbiornikami. Standard X1 jest oznaczeniem technologii transmisji wizji, fonii i sterowań oraz zasilania po jednej skrętce nieekranowanej, jak też oznaczeniem autonomicznego systemu wideofonowego, wykorzystującego ten standard. W obecnym systemie X1 można zastosować maksymalnie 4 panele wejściowe przyciskowe lub kodowe audio / wideo serii Targha oraz 64 aparaty odbiorcze (100 aparatów z panelem kodowym). Programowanie odbiorników odbywa się metodą uczenia i nie wymaga stosowania specjalistycznych narzędzi systemowych.

WYMAGANIA TECHNICZNE:

- Wywołanie rozmowy za pomocą jednego klawisza
- Komunikacja wizyjna i foniczna dwukierunkowa
- Rodzaj sygnału wizyjnego -kolor
- Możliwość otwarcia przejścia za pomocą przycisku unifonu (zwolnienie blokady SKD)
- Możliwość wywołania rozmowy z poziomu unifonów.

ZALECENIA

Elementy systemu komunikacji wizyjno- głosowej należy umieścić w pobliżu wejść pracowniczych zgodnie z rys. technicznym nr. PAS-120-PW-IT-SB-R-02-Rzut, Systemy Bezpieczeństwa - parter lub miejscu wytypowanym pod kątem wygody codziennej obsługi. Dobrana wysokość urządzeń musi zapewnić wygodę oraz zrozumiałą i wyraźną komunikację przez korzystające osoby. Wytypowane rozwiązanie musi zapewnić pełną integralność systemu z istniejącym rozwiązaniem funkcjonującym w pozostałych punktach komunikacyjnych Pałacu pod

kątem technicznym oraz ujednoliceniem obsługi administracyjnej systemu (zmiana parametrów pracy, rekonfiguracja ustawień etc.). Wymaga się podłączenie w nowo instalowanych panelach zewnętrznych układu sabotażowego podłączonego do systemu alarmowego. W przypadku braku możliwości technicznych (brak wbudowanego przełącznika /switcha) układ należy wyposażać w czujnik kontaktronowy bądź inne co najmniej adekwatne rozwiązanie pozwalające na sygnalizację otwarcia bądź oderwania obudowy od ściany.

18. SYSTEM REJESTRACJI CZASU PRACY

Projektuje się system oparty na rejestratorach RCP, które umożliwiają poprzez korzystanie z kart dostępu monitorowanie czasu pracy. System rejestracji czasu pracy powinien być zrealizowany z wykorzystaniem aktualnych osiągnięć technicznych w zakresie weryfikacji oraz identyfikacji tożsamości, zapewniając wysoką skuteczność oraz wygodę użytkownika. System rejestracji czasu pracy powinien być systemem sieciowym (rozproszonym), pracującym w architekturze klient-serwer. Klientem elementem systemu powinno być urządzenie, które pełni rolę terminala uwierzytelniającego, pozwalającego na pracę sieciową i/lub lokalną (np. gdy nie jest dostępne połączenie sieciowe). Terminal wykorzystuje połączenie sieciowe i protokoły rodziny TCP/IP dla celów komunikacji z elementem serwerowym. Element serwerowy pozwala na monitorowanie i zarządzanie więcej niż jednym elementem klienckim (rejestratorem). Należy zaprojektować i wdrożyć system Rejestracji Czasu Pracy bazujący na odczycie identyfikatora osoby w postaci karty zbliżeniowej z zapisem sektorowym, częstotliwości pracy 13,56 Mhz. System musi uwzględniać dwa niezależne punkty rejestracji, pracujące w charakterystyce sieciowej zgodnie z rzutem nr. PAS-120-PW-IT-SB-R-02-Rzut, Systemy Bezpieczeństwa – parter. Obsługa systemu będzie prowadzona z poziomu zdalnej aplikacji administracyjnej (WAN).

Główna jednostka rejestratora będzie wyposażona w dwa czytniki przypisane odpowiednio do wejścia i wyjścia pracowniczego z obiektu. Czytelny wyświetlacz ma za zadanie prezentować aktualny czas systemowy. Każdy z punktów będzie podłączony za pośrednictwem sieci LAN do serwera archiwizującego logi systemowe w trybie online.

W chwili obecnej w pałacu zainstalowane są dwa czytniki RCP. Każdy z nich ma możliwość zarejestrowania do 1000 kart pracowników.

Czytnik obsługuje rejestrację wyjścia(OT), wejścia(IN) oraz wyjścia służbowego(OS) (w nowych czytnika dobrze byłoby gdyby ten zakres rejestracji był większy).

Do czytników dołączona jest aplikacja Tango, która pozwala na programowanie czytników, zbieranie odczytów oraz nawadnianie bazy kart pracowników.

Czytniki przesyłają plik z odczytami na fizyczny komputer, który również znajduje się w Pałacu BN.

Format zapisu pliku według ustawień czytników nazywa się Adam.

Poniżej przykład pliku, który w takiej postaci przetwarzany jest w naszym systemie kadrowo-płacowym – rozszerzenie pliku to *.bin:

```
01 005467001560 01/03/17 05:02 IN 0000000000 0000
01 005467000143 01/03/17 05:03 IN 0000000000 0000
01 005467001440 01/03/17 05:08 IN 0000000000 0000
01 005467000006 01/03/17 05:10 IN 0000000000 0000
01 005467001441 01/03/17 05:10 IN 0000000000 0000
01 005467000632 01/03/17 05:10 IN 0000000000 0000
```

01- Oznacza numer czytnika

005467001560 – oznacza numer karty pracownika

01/03/17 - data odczytu

05:02 - godzina odczytu

IN (OT,OS) - rodzaj odczytu(w tym przypadku wejście,wyjście,wyjście służbwe)

W projektowanym systemie RCP plik z odczytami w opisanym powyżej formacie będzie eksportowany do udostępnionego za pomocą protokołu SMB folderu współdzielonego znajdującego się na stacji roboczej w pomieszczeniu służby ochrony. Nazwa folderu współdzielonego, uprawnienia do folderu współdzielonego oraz adres IP stacji do ustalenia z Zakładem Technologii Informatycznych. Stacja robocza służby ochrony podłączona będzie kablem ethernetowym do sieci LAN.

19. SYSTEM TELEWIZJI DOZOROWEJ (STD)

19.1.Opis stanu istniejącego

Obecnie funkcjonujący system STD oparto o urządzenia analogowe z zapisem cyfrowym na dysku HDD rejestratora. Obserwacja systemu ogranicza się do wybranych scen i pełni rolę wspomagającą prace służby ochrony. Dodatkową funkcjonalnością systemu jest stały zapis w trybie detekcji ruchu z poszczególnych punktów kamerowych. Podgląd systemu w trybie online jest dostępny dla pracownika monitoringu.

Realizacja projektu polega na całkowitym demontażu systemu wraz z towarzyszącą infrastrukturą kablową. Nowo zainstalowana struktura przewodowa będzie umożliwiać ponowne wykorzystanie i uruchomienie zdemontowanych urządzeń przy wykorzystaniu niezbędnych konwerterów dopasowujących parametry wejściowe sygnału analogowego z kamer do parametrów zastosowanej skrętki 6 kategorii. Docelowa wymiana na nowe urządzenia (rejestratory, switchy, kamery etc.) nastąpi w III etapie inwestycji. Dla tej części zadania Wykonwca ponownie zdemontuje całe wyposażenie i zainstaluje zaprojektowane urządzenia pozwalające na pracę we wskazanej funkcjonalności.

W ramach możliwości technicznych należy podłączyć istniejącą infrastrukturę (dotychczasowy rejestrator DVR) do systemu SMS w celu uruchomienia podstawowych funkcjonalności tj: obsługa systemu CCTV – odtwarzanie, zmiana trybu wyświetlania etc.

Szczegółowa lokalizacja montażu poszczególnych elementów w etapie II zostanie uzgodniona z Zamawiającym w trakcie prac instalacyjnych.

19.2.Charakterystyka STD projektowanego

Swoim zasięgiem obejmuje wewnętrzną oraz zewnętrzną część budynku. Część wewnętrzna pokryta polem obserwacji w zakresie wejścia do budynku biblioteki, korytarzy części biurowych i wystawowych, ciągów komunikacyjnych, przestrzeni otwartych, wyjść ewakuacyjnych oraz przestrzeni strefy wystawienniczej. W zakresie zewnętrznym pole obserwacji kamer ogranicza się do obserwacji elewacji na poziomie parteru z wejściami od strony Placu Krasińskich, ulicy Anielewicza oraz od strony ogrodu. System zewnętrzny dodatkowo pokrywa pobliskie otoczenie tj.: obszar parkingu, bram wjazdowych, części ogrodu oraz otoczenia będącego w strefie przy budynkowej.

W systemie STD zaimplementowano funkcję detekcji ruchu umożliwiającą dozоровanie zewnętrznej elewacji budynkowej. Każdorazowy ruch wykryty w określonym obszarze koreluje

zdefiniowane z systemem integrującym zdarzenia w celu wczesnego wykrycia zewnętrznego zagrożenia obiektu. Proponowany system musi uwzględniać topologię systemu TCP/IP opartą o technologię HD z zapisem cyfrowym na dyskach typu HDD. Zgodnie z wytycznymi oraz realnymi potrzebami użytkownika czas przechowywania nagrań zdarzeń określa się na minimalnie 30 dni. Konfiguracja podstawowa systemu musi umożliwiać operatorowi monitoringu następujące funkcjonalności:

- Przełączanie między punktami kamerowymi
- Pojedyncze urządzenie służące do zapisu obrazów ze wszystkich podłączonych do niego kamer, umożliwiać powinno zainstalowanie wewnątrz urządzenia dysków twardych o pojemności minimum 50 TB (zgodnie z poniższym wyliczeniem) umieszczonych w kieszeniach „hot swap”, z możliwością konfiguracji przestrzeni dyskowej przynajmniej w formie RAID 5 lub RAID 6 oraz dodatkowo podłączenie zewnętrznych macierzy dyskowych rozszerzających obsługiwaną pojemność dyskową do 256 TB
- Każde urządzenie powinno umożliwiać zapis i zarządzanie przynajmniej 128 kamerami
- Algorytm kompresji i dekompresji (w przypadku H.264) powinien umożliwiać niezależne definiowanie parametrów pracy dla każdego kanału (wejścia) wideo, z uwzględnieniem ustawienia długości struktury GOP lub częstości występowania klatek bazowych; zagwarantuje to dopasowanie do charakterystyki obserwowanej sceny i umożliwi dokładne definiowanie parametrów przepływności strumienia danych.
- Przełączanie zdefiniowanych multiwidoków
- Tworzenie i kasowanie multiwidoków dla własnego profilu.
- Podgląd w czasie rzeczywistym
- Podgląd materiału archiwalnego w całym zakresie
- Definiowania filtrów przeszukiwania archiwów tj.: czas, detekcja, wybrany punkt(y) kamerowe, wyszukiwanie po wskazanym obszarze nagranych materiału etc.
- Dla wybranych użytkowników istnieć musi możliwość zdefiniowania niezależnych ograniczeń co do podglądu na żywo i/lub odtwarzania pojedynczych kamer/grup kamer. Jednocześnie musi istnieć możliwość zdefiniowania maksymalnego wieku nagrań, jaki przysługuje użytkownikowi dla podglądu zarejestrowanego materiału (np. „użytkownik 1” może otworzyć wyłącznie materiał nie starszy niż 1 godzina)
- Zabezpieczenie nagranych materiału
- Sterowanie kamerami PTZ.

Lp.	Rodzaj kamery	Ilość klatek/bitrate	Średnia wielość zapisu	Ilość klatek/bitrate2	Średnia wielość zapisu 12 H
1	Zapis kl/sec.	1kl/s		12kl/s	
2	Kamera kopułowa 1080p	bitrate kb/s	GB/12h	bitrate kb/s	GB/12h
3		400	2,06	3072	15,82
4	Zapis ciągły kl/sec.	12kl/s		12kl/s	
5	Kamera obrotowa 1080p	bitrate kb/s	GB/12h	bitrate kb/s	GB/12h

6		4096	21,09	4096	21,09
7	Zapis kl/sec.	5kl/s	10kl/s		
8	Kamera 360 st 6MP	bitrate kb/s	GB/12h	bitrate kb/s	GB/12h
9		2048	10,55	5120	26,37

Lp.	Dobowa średnia wielkość zapisu	Miesięczna średnia wielkość zapisu	ilość kamer	Całkowita wielkość zapisu
1	GB/24h	GB/30dni	ilość kamer	TB/30dni
2	17,88	536,	87	45,57
3	GB/24h	TB/30dni	ilość kamer	TB/30dni
4	42,19	1,24	2	2,47
5	GB/24h	GB/30dni	ilość kamer	TB/30dni
6	36,91	1,08	3	3,24
7	Wymagana minimalna przestrzeń zapisu			51,29 TB

Tabela 17-1. Wielkość zapisu

Wykonawca zobowiązany jest do opracowania bilansu przestrzeni dyskowej na potrzeby zapisu obrazów z kamer STD i dopasowania pojemności dysków do przyjętego czasu archiwizacji (30 dni) i zastosowanych w trakcie realizacji urządzeń.

Jakość obserwowanego i archiwizowanego materiału wizyjnego musi zapewniać wymaganą obserwację dla sklasyfikowanych scen tj.:

- Elewację zewnętrzną;
- Wejścia główne i pomocnicze do obiektu;
- Korytarze komunikacyjne;

- d. Przestrzeń wystawiennicza stałą i czasową;
- e. Wejścia do poszczególnych stref administracyjnych i technicznych;
- f. Magazyny zbiorów;

W ramach wskazanych scen dozoru określa się odpowiednio cele i parametry dozoru w zakresie zalecanych minimalnych rozmiarów (osób) wyświetlanych na ekranach monitorów (wartości procentowe) dla zastosowanych w projekcie kamer megapikselowych (kamery o minimalnej rozdzielczości HD -1080p);

Tabela 19-2. Tabela konfiguracji celu i parametrów obrazu.

Cel obserwacji	Minimalny rozmiar	Typ sceny
Detekcja	10%	a)
Obserwacja	10%	a),e),d)
Rozpoznanie	20%	c),d)
Identyfikacja	40%	b), f)
Inspekcja	150%	a, b) kamery PTZ

Wymaga się utrzymania parametrów określonych w normie obrazów na granicach scen dozoru tzn. podane wartości muszą zostać spełnione przy obserwacji dla maksymalnych odległości, jakie obserwuje kamera:

- dla punktów kamerowych wewnętrznych - ściana przeciwna;
- dla punktów kamerowych zewnętrznych - odległość określona jako maksymalna odległość dozoru spełniająca założone cele.

CHARAKTERYSTYKA

W ramach projektu zastosowano kamery wyposażone w tryb dzień/noc z mechanicznym filtrem dla nocnych scen. Filtr przełączany zdalnie lub automatycznie dzięki sensorowi poziomu światła lub sterowany sygnałem wejściowym. Kamery oferują technologię Intelligent Dynamic Noise Reduction (iDNR) do redukcji szybkości danych i wymagań pamięci przez usuwanie wpływu szumu. Kamera zasilana przez Power over Ethernet (IEEE 802.3af) wyposażona w inteligentną analizę obrazu Intelligent Video Analysis (IVA) oraz analizę piksel po pikselu do automatycznej kompensacji światła wstecznego dla jasnych obszarów w wysoko kontrastowej scenie bez konieczności definiowania okna lub obszaru. Punkt kamerowy zapewnia inteligentną auto ekspozycję intelligent Auto Exposure (iAE) do zapewnienia czytelności wysoko kontrastowych scen (ciemne obiekty na jasnym tle i odwrotnie) i umożliwia pracę w słabo oświetlonych otoczeniach. Kamera używa technologii intelligent Dynamic Noise Reduction (iDNR) do aktywnej analizy zawartości sceny i konsekwentnej redukcji wpływu szumów. Kamera pozwala na pełną kontrolę i konfigurację przez sieć i jest zdolna do przechwycenia i przechowywania obrazów używając następujących standardów kompresji: H.264 MP (Profil główny) M-JPEG. Kamera powinna oferować dwukierunkową komunikację audio full duplex. Kamera musi posiadać możliwość konfiguracji w celu analizowania maks. 8 różnych algorytmów równoległe spośród dostępnych analizy poniżej:

- przekroczenia linii
- kierunkowość ruchu
- pozostawienia obiektu
- usunięcia obiektu
- podejrzanego zachowanie
- wykrycie twarzy
- sabotaż

- detekcja obiektu poruszającego się w przeciwnym kierunku
- Algorytm powinien mieć zaawansowane funkcje do kalibracji i monitorowania obiektu takie jak np. format obrazu, kierunek, kolor, obszar obiektu, prędkość.
- Dokładne lokalizacje kamer oraz sposób ich montażu Wykonawca uzgodni z Zamawiającym.

KAMERY ZEWNĘTRZNE.

Kamery zewnętrzne należy umieścić w osłonach hermetycznych o minimalnych parametrach środowiskowych dla klasy IV według PN-EN 50132, IP 65 oraz IK 10 z podgrzewaniem niezbędnym dla pracy w ujemnych temperaturach. Specyfika kamer i ich parametry zapobiegają prześwieceniu kamer w przypadku próby oślepienia. Funkcja WDR zapewnia dynamiczną zmianę poziomu oświetlenia sceny obrazu w zależności od punktowego „przeświecenia” lub nie doświecenia. Kamery stacjonarne wyposażone są w obiektywy z automatyczną przesłoną i regulowaną ogniskową, co umożliwia ustawienie kąta widzenia kamery po jej instalacji. Dodatkowo należy uwzględnić zastosowanie trybu auto regulacji focus punktów kamerowych w miejscach trudnodostępnych.

W celu zagwarantowania prawidłowej pracy kamer, Wykonawca zamontuje dodatkowe oświetlacze podczerwieni w przypadku gdyby sztuczne oświetlenie nocne nie zapewniało minimalnych parametrów niezbędnych do prawidłowego działania wybranego sprzętu.

KAMERY WEWNĘTRZNE/ZEWNĘTRZNE HEMISFERYCZNE

Kamery wytypowano z grupy kamer kopułowych z kątem obserwacji 360 stopni o minimalnych rozdzielczościach, co najmniej 5 Mipx. Kamera wyposażona w slot dodatkowej pamięci typu SD niezbędny do realizacji funkcjonalności awaryjnego zapisu oraz funkcję Dzień/Noc.

Konstrukcja kamery ma utrudniać możliwość celowej lub przypadkowej zmiany pola obserwacji, co w przypadku niskiego stropu poziomu piwnicy jest kwestią nadrzędną. Obserwacja pobliskiego otoczenia ma zapewnić nadzór możliwie największej przestrzeni wokół punktu obserwacyjnego, zapewniając jednocześnie pełną obserwację kluczowych punktów komunikacyjnych. Kamery zlokalizowane w zewnętrznej części stropowej balkonów należy umieścić w osłonach hermetycznych o parametrach środowiskowych, co najmniej dla klasy IV według PN-EN 50132, IP 65 oraz IK 10 z opcjonalnym podgrzewaniem lub właściwą konstrukcją niezbędną dla pracy w ujemnych temperaturach.

Wykonawca musi zapewnić zasilanie punktów kamerowych zgodne z ogólną koncepcją systemu STD (zasilanie PoE). W przypadku konieczności zastosowania grzałki należy dodatkowo doprowadzić przewód zasilający. Dokładne rozmieszczenie punktów kamerowych przedstawiono na rysunku nr PAS-120-PW –IT- CCTV-SCH-04-Schemat, System Telewizji Dozorowej.

KAMERY WEWNĘTRZNE.

Kamery znajdujące się w obiekcie zaprojektowano w wersji z oświetlaczami IR zapewniając dodatkową skuteczność kamery w przypadku braku oświetlenia bytowego. Należy wykorzystać kamery kuliste w wersjach wandaloodpornych, co uniemożliwi celowe lub przypadkowe przekręcenie kamery w celu zmiany jej pola widzenia.

STANOWISKA PODGLĄDU TELEWIZJI DOZOROWEJ (POMIESZCZENIE MONITORINGU)

W celu umożliwienia multi-obserwacji (np. przy pomocy dodatkowego pracownika ochrony) stref objętych monitoringiem zastosowano cztery dodatkowe monitory wielkoformatowe (o przekątnej minimum 40 cali) umieszczone w pomieszczeniu monitoringu na poziomie +2. Każdy z dwóch monitorów umożliwia wyświetlenie różnych konfiguracji obrazów z kamer. Przełączenie widoku/ów wykonuje operator monitoringu przy pomocy głównej aplikacji sterującej. Operator systemu STD ma możliwość niezależnego zdefiniowania wyświetlanego obrazu na każdym z nich z osobna. Pełna integralność systemu STD z aplikacją SMS musi umożliwiać dowolną integrację na poziomie softwarowym np. przypisanie wyświetlania obrazów z kamer lub uruchamiania presetów (kamery PTZ) dla danych przesyłanych do integratora z pozostałych systemów.

Do obsługi systemu monitoringu wykorzystywane będą 2 stacje robocze. Do każdej stacji podłączone będą po cztery monitory (2 wspomniane wcześniej o przekątnej minimum 40 cali i 2 umieszczone na biurku operatora o przekątnej minimum 24 cali).

System powinien obsługiwać dynamiczną transmisję strumieniową, w celu optymalizacji obciążenia sieci, obniżenia wymagań dla dekompresji obrazu i zwiększenia wydajności wyświetlania na stacjach podglądowych. W tym celu rozdzielczość transmitowanych "na żywo" obrazów powinna automatycznie dostosowywać się do rozmiaru (rozdzielczości) okien podglądu, w których wyświetlane są obrazy z poszczególnych kamer na stacji podglądowej. Dopasowanie to zależne powinno być od typu zastosowanej kamery, jednak system przy współpracy z wybranymi kamerami umożliwiać powinien automatyczne dopasowanie minimum do rozdzielczości: QCIF, QVGA, VGA, SVGA, WXGA, 720p, 1080p, 3MPix, 5MPix.

Użytkownik powinien mieć możliwość ustawiania takich parametrów, jak pozycja, rozmiar, kolor tła oraz czcionki, przy pomocy, których informacje te są wyświetlane – funkcjonalność ta umożliwi kilku użytkownikom ustawienie własnych preferencji wyświetlanych obrazów co podnosi poziom identyfikacji zdarzeń alarmowych.

Podgląd alarmowy (wywołanie sceny po wystąpieniu alarmu) powinien umożliwiać wyświetlenia pojedynczych obrazów przed- i po-alarmowych oraz całych sekwencji obrazów w pętli, dla jednej lub wielu kamer.

Zarządzanie zdarzeniami i alarmami powinno pozwalać na efektywną adaptację reakcji systemu na stany alarmowe oraz inne zdarzenia, zgodnie z wymaganiami użytkownika. Reakcje systemu powinny uwzględniać:

- Zdefiniowane przez użytkownika dowolnego czasu trwania sekwencji wideo przed i po wystąpieniu alarmu;
- Parametry rejestracji (jakość i przepływność) niezależne (indywidualne) dla wszystkich kamer;
- Automatyczne wyświetlanie obrazów alarmowych zdefiniowanych przez użytkownika (na żywo i/lub w trybie odtwarzania) na predefiniowanych stacjach roboczych;
- Wysyłanie informacji o alarmach lub zdarzeniach do zalogowanych użytkowników,
- Ustawienie jednej lub wielu kamer PTZ w zaprogramowanej pozycji;
- Rozpoczęcie tworzenia automatycznych kopii zapasowych predefiniowanych sekwencji w razie wystąpienia alarmu, bądź innego zdarzenia;
- Wysyłanie komunikatów email do zdefiniowanych adresatów, również z załączonymi obrazami alarmowymi.

PRZESTRZENŹ ZAPISU.

Charakterystyka przestrzeni objętych STD pod kątem wymagań dot. zapisu. W obiekcie wyróżniamy następujące kategorie pomieszczeń i przestrzeni, różniących się stopniem ryzyka zaistnienia niepożądanych zjawisk. Dla tych kategorii na bazie normy PN-EN 50132-7 oraz

wewnętrznych wymogów dla Biblioteki Narodowej przekazanych przez Zamawiającego w ramach wymagań użytkowych dobrano następujące parametry:

Wymagane prędkości rejestracji niezbędne do prawidłowego odtworzenia zapisanego obrazu. Zapisany obraz umożliwia rozpoznanie osób i ich identyfikację w wybranych miejscach.

- Wejścia do budynku – rozpoznanie osób za pomocą kamer umieszczonych przy wejściu. Identyfikacja odbywa się w strefie wejściowej - zapis z ciągłą prędkością minimum 5 kl./s przez czas otwarcia obiektu dla odwiedzających (przyjęto 12 godzin. Pozostały czas zapisu 3 kl./s).
- Kamery do identyfikacji zostały tak ustawione, żeby rozpoznawany obiekt zajmował, co najmniej 60% wysokości ekranu (dla rozdzielczości 720p) i 40% dla rozdzielczości Full HD.
- Otoczenie budynku: 6 kl./s przez cały czas.
- Wjazdy na teren otaczający obiektu: zapis 12,5 kl./s przez całą dobę w trybie detekcji ruchu.
- Prędkość rejestracji, rozdzielczość i jakość powinna być ustalana przez użytkownika niezależnie od parametrów strumieni do podglądu "na żywo". Konfiguracja powinna umożliwiać zmianę parametrów rejestracji „w locie” (bez konieczności zmiany parametrów kamery/kodera z aplikacji konfiguracyjnej – wcześniej predefiniowane parametry dla rejestracji) dla każdej kamery niezależnie, w różnych trybach pracy: nagrywanie ciągłe, nagrywanie zgodnie z harmonogramem czasowym oraz nagrywanie pre-alarmowe i alarmowe konfigurowane indywidualnie dla różnych typów zdarzeń alarmowych
- W celu niekontrolowanej utraty obrazu oraz zgodnie z obowiązującymi wymogami nie należy stosować opcji wydłużenia czasu archiwizacji materiału video w postaci zmiany ilości klatek już zarejestrowanego materiału – rozrzadzanie zapisu.

Szczegółowe parametry zapisu obrazu (ilość klatek referencyjnych, wielkość i typ baud rate, itp.) należy uzgodnić z Zamawiającym na etapie programowania STD.

Rejestracja sygnałów z kamer odbywała się w sposób cyfrowy. Archiwizowany materiał jest przetrzymywany na dyskach twardych znajdujących się w rejestratorze cyfrowym i na macierzach. Główny element magazynowy archiwum nagrań umiejscowiono w pomieszczeniu serwerowni na poziomie drugiego piętra w szafie rack. Dostęp do szafy posiadają dedykowani pracownicy – administrator systemów ochrony przebywając w pomieszczeniu monitoringu (lub czasowo obsługujący system). Biorąc pod uwagę powyższą charakterystykę i potrzeby obiektu należy wyliczyć niezbędną przestrzeń do zapisu dla minimum 30 dni przechowywania nagrań. Do wyliczeń sugeruje się wykorzystanie dedykowanego oprogramowania udostępnionego przez producenta na bazie kryteriów przytoczonych w normie EN 50132-7:2003 oraz wymogów funkcjonalno-technicznych Zamawiającego. System powinien udostępniać otwarte i udokumentowane interfejsy komunikacyjne. Producent systemu na żądanie powinien bezpłatnie udostępniać zestaw narzędzi programistycznych (z ang. Software Development Kit, SDK) oraz bezpłatne wsparcie programistów umożliwiające stworzenie oprogramowania integrującego z innymi systemami.

PRZELĄCZNIK SIECIOWY

W systemie przewidziano zarządzające przełączniki sieciowe, który zostały zamontowane w szafach współdzielonych z infrastrukturą IT na poziomach parteru oraz drugiego piętra. Przepustowość przełącznika zapewnia współpracę z serwerami i macierzami, które będą do niego wpięte.

Podstawowe parametry techniczne:

- Przełącznik zarządzający, warstwa 2
- przepustowość gigabit do wszystkich portów,

- nieblokowana architektura,
 - 4 porty SFP dla połączeń światłowodowych.
 - 24 porty,
 - Przepustowość 96 Gb/s,
 - Zarządzany, protokoły SNMP, RMON, CLI
- Szczegółowe wymagania pokazuje poniższa tabela:

Tabela 19-3. Szczegółowe wymagania dla przełącznika sieciowego

Standardy sieciowe	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x
Interfejsy fizyczne	24 x RJ-45 10BASE-T, 100BASE-TX, oraz 1000BASE-T
SFP	4 x Small form factor pluggable
Port konsoli	1 x RS232
Zarządzanie za pomocą 1 IP	do 48 przełączników
Metoda przekazywania ramek	Store-and-forward
Opóźnienie przełącznika	20 us dla 64-bajtowej ramki
Pamięć systemowa	128MB
Bufor	0,75 MB
Pamięć flash	32MB
Wielkość bazy MAC	8000
Ilość VLAN	1024
Ilość trunk	64
Ilość kolejek	8
Ilość statycznych tras	32
Ilość routowanych VLAN	32
Ilość wpisów ARPs	480
Ilość reguł ACL	224
Ramki Jumbo	do 9k
Emisja hałasu	do 38.6dB
Emisja cieplna	131.439 BTU
Interfejs użytkownika	CLI do 5 sesji, web z SSL / TLS, do 5 połączeń Telnet SSL
Diody LED	prękość, aktywność, połączenie, zasilanie, wentylator, RPS
Temperatura pracy	0-55 st. C

19.3. Zasilanie kamer.

Punkty kamerowe zamontowane we wskazanych na rysunkach punktach zasilono bezpośrednio napięciem 48 VAC z przełącznika sieciowego typu PoE, z dodatkowymi obwodami w przypadku zastosowania grzałek. Scentralizowane zasilanie podłączono do istniejących bezpieczników dedykowanych dla systemu STD w szafie energetycznej zgodnie z wymogami. Trasowanie wykonano uwzględniając konstrukcję budynku oraz zapewniając bezkolizyjność z innymi instalacjami. Wskazana trasa jest przejrzysta, prosta i dostępna do prawidłowej konserwacji

i remontów. Przy trasowaniu ciągów instalacji uniknięto dużej liczby skrzyżowań i zbliżeń z ciągami instalacji elektromagnetycznych i innymi instalacjami.

19.4. Funkcjonalność

System telewizji dozorowej zostanie podłączony do aplikacji integrującej typu SMS. Wygenerowane z systemu informacje alarmowe i techniczne będą zwizualizowane na mapie klienta PC w celu szybkiej oceny zdarzenie prowadzonej przez personel stanowiska monitoringu. Konfiguracja systemu musi zapewnić użytkownikowi zwizualizowanie i interakcję systemu SMS dla wykrycia ruchu w przestrzeni zewnętrznej elewacji:

- W postaci wyświetlenia obrazu z kamery wywołującej wskazane zdarzenie;
- Powstania sygnalizacji dźwiękowej (sygnalizacja dźwiękowa na komputerze klienta SMS)
- Ustawienia w zdefiniowany preset najbliższej kamery PTZ (obserwacja inspekcyjna auto/manual)

oraz powinien zapewnić w ramach przyszłej opcjonalnej rekonfiguracji systemu prowadzenie automatycznej dokumentacji nagrań w powiązaniu z zeskanowanymi kodami kreskowymi lub znacznikami RFID w celu zabezpieczenia np. zbiorów książkowych. Każde wydanie książki czytelnikowi po zeskanowaniu kodu kreskowego lub znacznika RFID musi umożliwiać automatyczną rejestrację obrazu i późniejszą możliwość przywołania tego zdarzenia np. po stwierdzeniu uszkodzenia książki lub zaginięcia wystarczy wprowadzić kod kreskowy, aby natychmiast otrzymać przegląd wszystkich powiązanych obrazów z kamer. Dzięki takiej funkcjonalności Właściciel będzie mógł wyeksportować materiał dowodowy i ustalić ostatnią osobę, która miała dostęp do książki lub elementu objętego funkcjonalnością związaną z kodami kreskowymi. Dla skutecznego wykorzystania wskazanej praktyczności rejestratora skanowanie kodów powinno odbywać się w strefie wydawania zbiorów Czytelnikowi jak i w strefie magazynowania w celu uzyskania pełnej dokumentacji wizyjnej. Dzięki pełnej integracji obrazów CCTV ze znacznikami zbiorów wyszukiwanie konkretnej książki nie sprawia najmniejszych trudności. Wszystkie dane znajdują się w jednym miejscu systemu, co znacząco ułatwia ustalenie powodów wystąpienia ew. nieprawidłowości.

19.5. Zapotrzebowanie mocy

Tabela 19-4. Zapotrzebowanie prądowe dla systemu CCTV

Lp.	Rodzaj	Moc urządzeń (W)	szt.	Maksymalna moc całkowita (W)
1	Rejestrator cyfrowy	410	1	410
2	Switch sieci szkieletowej	380	1	380
3	Switch 1	380	1	380
4	Switch 2	380	1	380
5	Switch 3,4	380	2	760
6	Switch 5,6	380	2	760
7	Grzałki do zewnętrznych punktów kamerowych	25	10	250
8	Zapotrzebowanie całkowite (W)			3320

Tabela 19-5. Zapotrzebowanie prądowe dla stanowiska integratora

Lp.	Rodzaj	Moc urządzeń (W)	Szt.	Maksymalna moc całkowita (W)
1	Stanowisko PC	600	1	600
2	Monitor LCD/LED	50	4	200
3	Zapas na opcjonalne dodatkowe wyposażenie	500	1	500
4	Zapotrzebowanie całkowite (W)			1300

Wykonawca zobowiązany jest do opracowania bilansu energetycznego STD i dopasowania pojemności akumulatorów do przyjętego czasu podtrzymania i zastosowanych w trakcie realizacji instalowanych urządzeń.

20. INTEGRATOR SYSTEMÓW (SMS)

20.1. Założenia ogólne

Dla potrzeb ujednolicenia interfejsu obsługi, prezentacji zbiorczych informacji i szybkiej migracji zdarzeń pomiędzy systemami bezpieczeństwa projektuje się podłączenie systemów ochrony technicznej do platformy SMS opartej o otwarte rozwiązanie softwarowe typu Security Management System. Jest to platforma pozwalająca na wszechstronne, wydajne, łatwe w użyciu zarządzanie bezpieczeństwem, które można łatwo zintegrować z infrastrukturą IT. Projektowana platforma zapewnia integrację aplikacji bezpieczeństwa i ujednolicenia systemów bezpieczeństwa, w tym systemu sygnalizacji włamania i napadu, kontroli dostępu, telewizji dozorowej. Wszystko w ramach jednej platformy zarządzania bezpieczeństwem bez konieczności połączeń sprzętowych. Wykonawca systemu SSWiN musi udostępnić przez interfejs TCP/IP wszystkie sygnały potrzebne do prawidłowej integracji lub innym alternatywnym medium.

Projekt dopuszcza wykorzystanie dowolnego rozwiązania wykorzystującego wskazane poniżej funkcjonalności zapewniając jednocześnie przesyłanie wszystkich sygnałów i korelacji pod kątem zapewnienia pełnej zgodności ze wskazanymi normami dla poszczególnych systemów.

20.2. Zakres integracji sprzętowej.

Integracja z wykorzystaniem interfejsu TCP/IP – pełen dostęp do sygnałów generowanych przez systemy.

20.3. Zalecenia dla integracji z systemami bezpieczeństwa.

- Sygnał alarmowy (napad, włamanie, sabotaż) - Przywołanie obrazu z najbliższych kamer w strefie alarmowej;
- Opcjonalnie zazbrojenie strefy alarmowej powoduje blokadę czytników dostępowych systemu kontroli dostępu realizujących funkcje przejścia do tej strefy;
- Alarm ze strefy w zależności od miejsca jego powstania, powoduje wyświetlenie komunikatu dla obsługi o koniecznych do przeprowadzenia czynnościach zgodnie z ustaloną procedurą. Komunikat alarmu musi zostać potwierdzony przez operatora;

20.4. Zalecenia dla wykonania wizualizacji.

- Wizualizowanie stanów alarmowych wszystkich detektorów w tym alarm, sabotaż;
- Wizualizowanie stanów alarmowych ze stref;
- Wizualizowanie stanów zazbrojenia i rozbrojenia stref;
- Wizualizowanie sygnałów technicznych: awarii zasilaczy, detektorów oraz charakterystycznych punktów infrastruktury integralnej np.: brak zasilania switchy, urządzeń gablot etc.
- Stan komunikacji z centralą alarmową, kontroli dostępu oraz systemem monitoringu;

20.5. Ogólne zalecenia montażowe systemów bezpieczeństwa

20.5.1. Prowadzenie instalacji

Wszystkie trasy kablowe znajdujące się poza głównym dedykowanym do instalacji zabezpieczeń szachtem kablowym (koryta podłogowe, ciągi komunikacyjne między stropowe etc.) należy układać w osłonach PCV podtynkowo. Zastosowane materiały muszą uwzględnić możliwość położenia nowego i miarę możliwości dołożenia dodatkowego okablowania w trasach kablowych przewidzianych do późniejszych modyfikacji np. okablowanie kamer hemisferycznych zewnętrznych – drzwi główne (centralne) od strony parku i ul Plac Krasińskich. Wymaga się zastosowanie rurek typu RHDPE z powłoką poślizgową lub innego nie gorszego, alternatywnego rozwiązania bazując na dostępnych technicznych możliwościach ułożenia okablowania np. wdmuchiwanie przewodów oraz stosowania minimalnych promieni skrętów. Wszystkie trasy muszą być wykonane w sposób estetyczny i umożliwiający wykonanie prac naprawczych. Nie dopuszcza się trasowania bruzd w narożnikach pomieszczeń oraz w bezpośrednio w miejscach ozdobnych (wskazanych, jako elementy wystroju „muzealnego”). Wszystkie przewierty, miejsca montażu wyposażenia systemów bezpieczeństwa oraz wskazane trasy kablowe na etapie wykonawczym muszą uzyskać akceptację konserwatora. W ramach ogólnych wytycznych rekomenduje się prowadzenie tras oraz montażu elementów o charakterze niezakłócającym wystroju obiektu.

Roboty podstawowe: montaż instalacji i urządzeń należy wykonać niżej wymienione prace z zachowaniem podanych zaleceń:

- Na styku (skrzyżowania i zbliżenia) z innymi instalacjami należy stosować odcinki rurek lub inne przekładki izolacyjne.
- Należy koordynować przebieg tras kabli danej instalacji oraz innych instalacji i zachować następujące minimalne odstępów równoległych linii kablowych:
 - 20 cm od przewodów energetycznych przy braku przegrody,
 - 5 cm od przewodów energetycznych zastosowaniu przegrody stalowej (np. korytka),
 - 30 cm od opraw oświetleniowych typu „światłówka”,
 - 100 cm od transformatorów i silników zgodnie z normą PN-EN 50174-2:2010.
- Nie wykonywać żadnych połączeń przewodów poza tymi, które wskazuje projekt.
- Minimalny promień gięcia wg określenia producenta lub co najmniej 8-krotna średnicy kabla.
- Nie wolno wykonywać nadmiarowych połączeń przewodów.

UWAGA:

Wskazane na planach instalacji lokalizacje elementów systemu mogą ulec zmianie na skutek:

- Wprowadzenia zmian architektonicznych;
- Zmian ustawienia wyposażenia;
- Zmian przeznaczenia pomieszczenia.

W tym zakresie dopuszcza się indywidualne „maskowanie” urządzeń za pomocą malowania poszczególnych detektorów, czujników czy też obudów kamer.

W zakresie zabezpieczenia pozostałych elementów infrastruktury wyposażenia technicznego obiektu zaleca się zabezpieczenia szachtów technicznych oraz wjazdu zewnętrznego czujnikami otwarcia (kontaktronami). Element zewnętrzny sygnalizujący otwarcie studzienki teletechnicznej należy wykonać w charakterystyce odseparowania galwanicznego dla pozostałej części systemów ochrony technicznej lub przy pomocy niezależnego systemu detekcyjnego typu dodatkowa podcentrala alarmowa. Infrastruktura sieciowa w zakresie sieci Security (punkty BPD) powinna być zabezpieczona czujnikami sygnalizującymi otwarcie szafy rack dla każdego ruchomego skrzydła tj. należy zabezpieczyć czujnikami kontaktronowymi każdą z szafek rack czujnikiem sygnalizującym otwarcie każdego ruchomego skrzydła.

Przejścia przez ściany i stropy powinny spełniać następujące wymagania:

- wszystkie przejścia obwodów instalacji elektrycznych przez ściany, stropy itp. są chronione przed uszkodzeniami,
- przejścia wykonane w przepustach rurowych,
- przejścia pomiędzy pomieszczeniami o różnych atmosferach wykonywać w sposób szczelny, zapewniający nie przedostawanie się wycieków,
- przejścia pomiędzy strefami pożarowymi zabezpieczyć ochroną bierną. Przepusty instalacyjne w elementach oddzielania przeciwpożarowego powinny mieć odporność ogniową (EI) wymaganą dla tych elementów.
- Sprzęt i osprzęt instalacyjny należy mocować do podłoża w sposób trwały zapewniający mocne i bezpieczne jego osadzenie.

20.5.2. Zabezpieczenie antysabotażowe

Wszystkie urządzenia, puszki połączeniowe, przewody systemu alarmowego należy zabezpieczyć antysabotażowo tzn., że każda próba rozkręcenia obudowy dowolnego urządzenia lub przecięcia przewodu powinna natychmiast wywołać alarm sabotażowy bez względu na to, czy system jest włączony w dozór czy nie. Zaleca się wykonywanie minimalnej i niezbędnej ilości puszek łączeniowych bazując na łączeniach wykonywanych wewnątrz samych urządzeń np. łączenie magistrali sygnałowych wewnątrz czujników adresowalnych.

20.5.3. Wykonanie okablowania systemu

Do wykonania instalacji projektuje się następujące typy przewodów w wersji bezhalogenowej:

- przewód YSTY 2x2x0.8 – magistralny,
- przewód UTP 4x2x0,5 kat. 6 – linii dozorowych konwencjonalnych i cyfrowych,
- kabel UTP kat.6 – ziemny, żelowany – linii dozorowych konwencjonalnych dla urządzeń montowanych na zewnątrz,
- przewód NHXH 3x1,5 – zasilanie 230V

W ramach prac związanych z okablowaniem systemu zarówno po stronie zasilającej jak i po stronie sygnałowej należy uwzględnić odpowiednie przekroje przewodów mając na uwadze spadki napięć oraz wymagane parametry impedancyjne. Pod uwagę należy wziąć realną długość przewodów (pętli magistralowych urządzeń adresowalnych, elementów analogowych (klasyczne

kontaktrony, czujnik, detektory oraz sygnalizatory) oraz długości krytyczne w zakresie urządzeń IP nie dopuszczając do spadku poniżej zalecanej przez producenta wartości i obowiązujących norm.

Przewody należy układać w strefach między stropowych w wyznaczonych trasach koryt kablowych przeznaczonych dla instalacji bezpieczeństwa.

Ze względu na prowadzenie prac w działającym i wykończonym obiekcie dokładną trasę i sposób wykonania należy ustalać w trakcie realizacji. Wykonanie okablowania i montaż urządzeń musi zostać wykonany w sposób estetyczny. Wszystkie elementy systemu należy zamontować i połączyć zgodnie z DTR-kami urządzeń.

Zasilanie podstawowe

Dla poszczególnych systemów zostaną przewidziane osobne układy zasilające 230V/50Hz określone w projekcie elektrycznym. Każdy z nich będzie zabezpieczony pod kątem przeciwzwarciovym oraz przeciw porażeniowym. W ramach projektu systemu zabezpieczeń wskazuje się podłączenie systemu do dedykowanego obwodu odpowiednim przewodem zasilającym tor zasilania podstawowego.

20.5.4. Prowadzenie okablowania systemowego pod tynkiem

Rury RHDPE podtynkowo (poza główną trasą koryt/kanałów metalowych) dla kabli instalacji teletechnicznych i elektrycznych należy wykonać mając na uwadze zapewnienie odpowiedniego promienia zgięcia kabli nie mniejszego niż określony przez ich producenta (zgodnie z kartą katalogową) przewidzianego do stosowania kabla. Koniecznym jest także unikanie wszelkich zbliżeń do instalacji energetycznych. Powinny być zachowane minimalne odstępki określone dla danego typu instalacji w odpowiednich normach.

20.5.5. Inne zalecenia

Stosowanie rur kablowych wraz z preinstalowaną linką zaciągową (tzw. „pilot”).

Ciągi instalacji teletechnicznych należy umieszczać poniżej instalacji elektroenergetycznych.

Po wciągnięciu kabli wszelkie przepusty rurowe, a zwłaszcza przepusty przez stropy i ściany na granicach stref pożarowych, powinny być uszczelnione przy użyciu certyfikowanych materiałów np. mas ogniochronnych pęczniących pod wpływem temperatury, przegród ogniochronnych (w pionach dla umożliwienia rozbudowy wiązek kabli), zapraw ogniochronnych, osłon ogniochronnych, bloczków ogniochronnych, poduszek ogniochronnych (przeznaczonych do wtórnej zabudowy, np. po rozbudowie wiązki kabli) itp.

Sukcesywnie po ułożeniu okablowania należy odtworzyć stan sprzed wykonywania robót.

20.5.6. Układanie kabli

Parametry transmisyjne kabli symetrycznych (UTP, YTKSY) są osiągnięte poprzez zachowanie odpowiednich separacji i układu pomiędzy poszczególnymi parami w tych kablach. Dlatego dla niezmiennego zachowania tych parametrów istotne jest restrykcyjne przestrzeganie poniższych reguł instalacyjnych:

Należy wystrzegać się nadmiernego ściskania kabli (np. podczas upinania opaskami kablowymi w wiązki), deptania po kablach ułożonych na podłodze oraz załamywania kabli na elementach konstrukcji kanałów kablowych itp.. Przy odwijaniu kabla z bębna bądź wyciąganiu kabla z pudełka nie należy przekraczać maksymalnej siły ciągnięcia oraz zwracać uwagę na to, by na kablu nie tworzyły się węzły ani supły. Przy prowadzeniu kabli w kanałach kablowych należy różne rodzaje kabli układać w oddzielnych przegrodach kanału. Trasując i rowkując okablowanie poza głównymi szachtami kablowymi należy uwzględnić trasy bazując na minimalizacji wykonywanych

zniszczeń wystrzegając się wykonywania przewiertów, rowkowania w pobliżu elementów wystroju obiektu. Przed przystąpieniem do właściwego układania tras kablowych i kabli wykonawca wykona wstępny plan tras i uzyska zezwolenie na wykonanie przewiertów, nawiertów, przepustów i rowkowania w architekturze budynku. Podstawą do planowania tras będzie w miarę możliwości utrzymanie kolejności (adresowania) elementów wskazanych na rzutach i rysunkach technicznych. Dopuszcza się zmiany w konfiguracji tras pod warunkiem utrzymania parametrów technicznych i granicznych instalacji przewodowej (długości graniczne).

Końcowe odcinki tras kablowych i podejścia do odbiorników prowadzić podtynkowo w ścianach z użyciem gładkościennych rur elektroinstalacyjnych RHDPE.

W pomieszczeniach ze zdobieniami kable i przewody prowadzić w przestrzeni tła i w sposób jak najmniej ingerujący w dekoracyjne wykończenie pomieszczeń. Wszelkie uszkodzenia należy odtworzyć.

20.5.7. Uziemienie i ekranowanie

Podstawowym celem uziemienia jest zapewnienie bezpieczeństwa, czyli ograniczenie możliwości dotyku i zapewnienie ścieżki powrotnej w przypadku uszkodzenia uziemienia, a także zapewnienie ochrony EMC: zerowego potencjału odniesienia i wyrównania napięć, efektu ekranowania. W celu uzyskania najlepszych rezultatów, system uziemiający powinien być połączony w trzech wymiarach, w szczególności w przypadku wielokondygnacyjnych budynków wyposażonych w sieciowy system przesyłania danych. Należy pamiętać, że jednym z największych niebezpieczeństw jest indukowanie się przepięciowych pól magnetycznych w pętach zwarciovych do ziemi. Pole przepięciowe jest głównie poziome i indukuje najgorsze błędzące napięcia w pionowych pętach.

W przypadku instalacji systemów ekranowanych należy zastosować się do następujących wskazówek:

- wszystkie elementy systemu muszą być ekranowane i pochodzić od jednego producenta,
- gwarantuje to niską impedancję przejścia,
- podłączenie ekranów kabli musi gwarantować ciągłość i skuteczność ekranu,
- ekran musi być ciągły na całym odcinku kabla, nie wolno przerywać ekranu,
- należy zwrócić szczególną uwagę na montaż elementów połączeniowych. Kontakt ekranu powinien występować na całym obwodzie, połączenie do ziemi powinno być wykonane w sposób trwały i gwarantujący ciągłość.

Wymaga się w przypadku urządzeń zewnętrznych (kamery STD) zastosowania zabezpieczeń przeciwprzepięciowych zabezpieczających elementy infrastruktury przed wyładowaniami elektrostatycznymi w formie adekwatnej do proponowanego rozwiązania (tor transmisji sygnału, zasilanie PoE, zasilanie grzałek 230 V/12 V). Instalacja musi posiadać zabezpieczenie każdej linii zewnętrznej osobnym układem zabezpieczającym dany tor kablowy zgodnie z normami oraz stosowaną praktyką.

20.5.8. Próby montażowe

Zakres nadzoru prób i pomiarów nad robotami elektrycznymi powinien być wykonywany zgodnie ze szczegółami podanymi w niniejszej specyfikacji oraz z ogólnymi Warunkami Technicznymi Wykonania i Odbioru Robót Budowlanych. Zakres podstawowych prób obejmuje:

- pomiary transmisyjne dedykowane dla określonych kabli teletechnicznych;
- pomiary elektryczne gniazd zasilających urządzenia teletechniczne;
- próby zadziałania wyłączników różnicowoprądowych urządzeń teletechnicznych;
- pomiary instalacji wyrównawczej, uziemiającej i odgromowej.

Pomiary powinny być zakończone protokołem i zawierać:

- a) miejsce wykonania pomiarów,
- b) datę wykonania,
- c) rodzaj, typ i numer miernika, data ważności kalibracji
- d) zakres pomiarów, wyszczególnienie odcinków pomiarowych
- e) wyniki pomiarów poddane analizie,
- f) ocenę stanu instalacji oraz informacje, które według Wykonawcy mogą mieć znaczenie w ocenie stanu faktycznego.

20.5.9. Czynności i prace odbiorowe

Odbiór instalacji należy przeprowadzić po 3 tygodniach pracy próbnej systemu alarmowego. Przy odbiorze systemu należy przeprowadzić badania mechaniczne i elektryczne, w szczególności:

- Sprawdzenie (ogłędziny) materiałów w zakresie zgodności z obowiązującymi przepisami i Projektem Wykonawczym;
- Sprawdzenie wykonania systemów SSWiN w zakresie zgodności z Projektem Wykonawczym, ze szczególnym uwzględnieniem:
 - Wykonania połączeń;
 - Zamocowania urządzeń i osprzętu;
 - Zainstalowania właściwych elementów;
 - Próby okablowania na przerwy i zwarcia między żyłami danego kabla;

Sprawdzenie protokołów pomiarowych

- Sprawdzenie czy system alarmowy jest w stanie gotowości do pracy;
- Sprawdzenie poprawności działania wszystkich elementów, łącznie z urządzeniami uruchamianymi ręcznie (czujniki alarmowe, przyciski napadowe, styki sabotażowe itp.);
- Sprawdzenie zgodności z wymaganiami wszystkich połączeń giętkich;
- Sprawdzenie poprawności działania central alarmowych, serwerów, rejestratorów, modułów rozszerzeń, zasilaczy;
- Sprawdzenie poprawności działania każdego elementu;
- Sprawdzenie czy system a jest w stanie gotowości do pracy.

Przed przekazaniem instalacji do odbioru, Wykonawca zobowiązany jest dostarczyć Inwestorowi dokumentację powykonawczą zawierającą:

- a) Zaktualizowany projekt wykonawczy z naniesionymi zmianami powstałymi w czasie montażu oraz uzgodnieniami roboczymi dotyczącymi zmian;
- b) Kopie konfiguracji systemów na nośniku elektronicznym np. CD,DVD uniemożliwiającym przypadkowe skasowanie danych i utratę kopii zapasowych wszystkich ustawień systemów;
- c) Protokoły z pomontażowych prób i testów;
- d) Protokoły pomiarowe;
- e) Protokoły odbiorów częściowych;
- f) Certyfikaty zainstalowanych urządzeń;
- g) Niezbędne poświadczenia zgodności na wszystkie urządzenia i podsystemy oraz produkt jako jednolita struktura security;
- h) Protokoły ze szkolenia obsługi;
- i) Wypełnioną książkę eksploatacji systemu.

Odbiorowi podlegać będzie również estetyka wykonania prac.

20.5.10. Szkolenie

Przedstawiciel Wykonawcy przeszkoli personel w zakresie budowy urządzeń, ich pracy, ustawienia wszystkich elementów sterowania, bezpieczeństwa i kontroli, przekaze on również wszelkie informacje niezbędne dla zapewnienia bezawaryjnej pracy i codziennej obsługi instalacji. Wykonawca przekaze również materiały szkoleniowe, których zakres zostanie uzgodniony z Zamawiającym.

Szkolenie musi obejmować:

- konfigurację systemu,
- obsługę systemu,
- programowanie danych użytkownika (dodawanie, usuwanie, zmianę uprawnień),
- obsługę alarmów.
- generowanie raportów
- programowanie zmian systemu

Po zakończeniu szkoleń Wykonawca zobowiązany jest przekazać kompletne instrukcje obsługi i konserwacji dla wszystkich instalacji oraz wystawić zaświadczenia o ukończeniu szkolenia dla osób w nim uczestniczących.

20.5.11. Eksploatacja i konserwacja systemu.

Zgodnie z dobrą praktyką oraz wymogami dotyczącymi obsługi systemów ochrony należy wykonywać okresowe przeglądy działania elementów systemu. Czyszczenie elementów optycznych kamer i obudów jest zalecane, co 3 miesiące dla kamer wewnętrznych oraz zewnętrznych. System należy okresowo poddawać konserwacji, zgodnie z harmonogramem dostarczonym przez dostawcę. Przed przystąpieniem do zabiegów konserwacyjnych należy sprawdzić kalibrację urządzeń pomiarowych. Jeżeli podczas konserwacji muszą być przeprowadzone badania okresowe, informacja o tym fakcie powinna być zapisana w harmonogramie. W czasie trwania zabiegów konserwacyjnych powinien być zapewniony dostęp do odpowiednich części zamiennych po to, aby możliwe było przeprowadzenie niezbędnych napraw. Wyniki testów okresowych należy rejestrować. Konserwacja i testowanie powinny być wykonywane wyłącznie przez wykwalifikowany personel.

21. UWAGI KOŃCOWE

Wykonawca w ramach niniejszego zakresu robót wykona wszystkie prace nieopisane w tym dokumencie, a które są niezbędne do prawidłowego zakończenia robót oraz te, które ze względu na swoją wiedzę fachową uzna za stosowne po wcześniejszym uzgodnieniu z projektantem i Zamawiającym. Wszystkie prace wykonywane w zakresie nowo dostarczonych elementów muszą być wykonywane przez gwaranta lub osoby przez niego wyznaczonej.

Zgodnie ogólnie przyjętymi zasadami i powszechnie stosowaną praktyką:

- Instalację należy wykonać zgodnie z obowiązującymi normami, przepisami i zasadami wiedzy technicznej;
- Instalacja powinna pozostawać pod stałym nadzorem firmy prowadzącej konserwację;
- Firma wykonująca instalację i/lub prowadząca serwis pogwarancyjny dokona przeszkolenia personelu Użytkownika w zakresie obsługi instalacji oraz opracuje instrukcje postępowania w przypadkach wystąpienia alarmów. Instrukcje te powinny być wywieszone w punkcie nadzoru;
- Wykonawca jest zobowiązany do kompletnego wykonania instalacji i zapewnienia jej pełnej funkcjonalności poprzez zastosowanie koniecznych materiałów i urządzeń;

- Końcowe odcinki tras kablowych i podejścia do odbiorników prowadzić podtynkowo w ścianach z użyciem gładkościennych rur elektroinstalacyjnych RHDPE.
- W pomieszczeniach ze zdobieniami kable i przewody prowadzić w przestrzeni tła i w sposób jak najmniej ingerujący w dekoracyjne wykończenie pomieszczeń. Wszelkie uszkodzenia należy odtworzyć.
- Wykonawca zobowiązany jest do takiego zaprogramowania systemu, aby wykorzystać wszystkie możliwości, które daje proponowana platforma sprzętowa i programowa. Wszelkie prace należy prowadzić w ścisłej współpracy i wg wytycznych Inwestora;
- Wszelkie nazwy własne produktów i materiałów przywołane w projekcie, służą określeniu pożądanego standardu wykonania i określeniu właściwości oraz wymogów technicznych założonych w dokumentacji technicznej dla danych rozwiązań;
- W przypadku, gdy Wykonawca zastosuje urządzenia niezgodne z wymaganiami będzie obciążony kosztami demontażu, zakupu i montażu urządzeń spełniających wymagania niniejszej dokumentacji;
- Rysunki i część opisowa są dokumentacjami wzajemnie uzupełniającymi się. Wszelkie wątpliwości należy rozstrzygnąć na korzyść Zamawiającego;
- Wszelkie wykonywane prace oraz proponowane materiały winny odpowiadać Polskim Normom i posiadać stosowną deklarację zgodności lub posiadać znak CE i deklarację zgodności z normami zharmonizowanymi oraz posiadać niezbędne atesty tak aby spełniać obowiązujące przepisy;
- Niezależnie od dokładności i precyzji dokumentów otrzymanych od Inwestora, definiujących usługę do wykonania, Wykonawca zobowiązany jest do uzyskania dobrego rezultatu końcowego. W związku z tym wykonane instalacje muszą zapewnić utrzymanie założonych parametrów technicznych. W przypadku rozbieżności, Wykonawca winien wyjaśnić z Inwestorem, który jako jedyny jest upoważniony do wprowadzenia zmian;
- Wszelkie instalacje kablowe przechodzące przez przegrody p.poż. muszą zostać zabezpieczone uszczelnieniem p.poż. Prace te należy wykonywać, gdy sama instalacja jest już ukończona. Uszczelnienie należy wykonać zgodnie z polskimi normami, stosownymi przepisami i aprobatami
- Po oddaniu systemu do eksploatacji należy wykonywać nie rzadziej jak raz na 3 miesiące konserwację;
- Wszelkie prace związane z konserwacją, modernizacją lub naprawą systemów należy zapisać w książkach eksploatacji każdego z systemów .

Zamawiający zastrzega sobie prawo do wykonywania rozbudowy systemów powstałych w ramach inwestycji bez utraty gwarancji, pod warunkiem wykonywania prac związanych z rozbudową przez osoby posiadające kwalifikacje i uprawnienia określone w przepisach prawa ogólnie obowiązującego.

W trakcie wykonywania prac, na każdorazowe odstępstwa od projektu wykonawczego oraz w przypadku istotnych zmian materiałowo- koncepcyjnych przed przystąpieniem do prac należy uzyskać akceptację użytkownika przestrzeni, projektanta oraz konserwatora zabytków.

SPIS ZAŁĄCZONYCH RYSUNKÓW

Lp	Numer	Tytuł
1	PAS-120-PW-IT-LAN-R-01_E_II_2.3	Instalacja okablowania strukturalnego LAN, WiFi – piwnica
2	PAS-120-PW-IT-LAN-R-02_E_II_2.3	Instalacja okablowania strukturalnego LAN, WiFi – parter
3	PAS-120-PW-IT-LAN-R-03_E_II_2.3	Instalacja okablowania strukturalnego LAN, WiFi – 1 piętro
4	PAS-120-PW-IT-LAN-R-04_E_II_2.3	Instalacja okablowania strukturalnego LAN, WiFi – 2 piętro
5	PAS-120-PW-IT-LAN-R-05_E_II_2.3	Instalacja okablowania strukturalnego LAN, WiFi – poddasze
6	PAS-120-PW-IT-SB-R-01_E_II_2.3	Systemy bezpieczeństwa – piwnica
7	PAS-120-PW-IT-SB-R-02_E_II_2.3	Systemy bezpieczeństwa – parter
8	PAS-120-PW-IT-SB-R-03_E_II_2.3	Systemy bezpieczeństwa – 1 piętro
9	PAS-120-PW-IT-SB-R-04_E_II_2.3	Systemy bezpieczeństwa – 2 piętro
10	PAS-120-PW-IT-SB-R-05_E_II_2.3	Systemy bezpieczeństwa – 3 piętro
11	PAS-120-PW-IT-SSP-R-01_E_II_2.3	Instalacja SSP – piwnica
12	PAS-120-PW-IT-SSP-R-02_E_II_2.3	Instalacja SSP – parter
13	PAS-120-PW-IT-SSP-R-03_E_II_2.3	Instalacja SSP – 1 piętro
14	PAS-120-PW-IT-SSP-R-04_E_II_2.3	Instalacja SSP – 2 piętro
15	PAS-120-PW-IT-SSP-R-05_E_II_2.3	Instalacja SSP – poddasze
16	PAS-120-PW-IT-SSP-SCH-01_E_II_2.3	Schemat – instalacja SSP
17	PAS-120-PW-IT-CSO-SCH-02_E_II_2.3	Schemat systemu oddymiania
18	PAS-120-PW-IT-SKD-SCH-03_E_II_2.3	Schemat – instalacja KD
19	PAS-120-PW-IT-CCTV-SCH-04_E_II_2.3	Schemat – system telewizji dozorowej
20	PAS-120-PW-IT-SSWiN-SCH-05_E_II_2.3	Schemat – instalacja SSWiN
21	PAS-120-PW-IT-PRYZ-SCH-06_E_II_2.3	Schemat – instalacja przyzywowa
22	PAS-120-PW-IT-LAN-SCH-07_E_II_2.3	Schemat okablowania strukturalnego LAN, WiFi
23	PAS-120-PW-IT-LAN-SCH-08_E_II_2.3	Schemat – szafy RACK BPD-11, BPD-12, BPD-13, BPD-14, PS, TSM1, TSM2
24	PAS-120-PW-IT-LAN-SCH-09_E_II_2.3	Schemat – szafa RACK BPD-21
25	PAS-120-PW-IT-LAN-SCH-10_E_II_2.3	Schemat – szafa RACK BPD-31
26	PAS-120-PW-IT-LAN-SCH-11_E_II_2.3	Schemat – budynkowy punkt styku
27	PAS-120-PW-IT-LAN-SCH-12_E_II_2.3	Schemat – telefoniczna centrala abonencka

mgr inż. Piotr Wudarczyk
 Uprawnienia budowlane do projektowania
 i kierowania robotami budowlanymi
 bez ograniczeń w specjalności instalacyjnej
 w zakresie sieci, instalacji i urządzeń
 elektrycznych i elektroenergetycznych
 nr ewid. M/22 0424/PWOE/06

mgr inż. Michał Niedźwiecki
 Uprawnienia budowlane do projektowania
 bez ograniczeń w specjalności instalacyjnej
 w zakresie sieci, instalacji i urządzeń
 elektrycznych i elektroenergetycznych
 nr ewid. WAM/0140/PWOE/05

ZAŁĄCZNIKI

UPRAWNIENIA I ZAŚWIADCZENIA PROJEKTANTÓW



sygn. akt. MAZ/7131-7132/ 526 /06 /E

Warszawa, dnia 29 grudnia 2006 r.

DECYZJA

Na podstawie art. 11 ust. 1 i art. 24 ust. 1 pkt 2 ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów, inżynierów budownictwa oraz urbanistów (Dz.U. z 2001 r. Nr 5 poz. 42 z późn. zm.), art. 12 ust. 1 pkt 1-5, ust. 3, art. 13 ust. 1, 3 i 4, art. 14 ust. 1 pkt 5 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (tekst jedn.: Dz.U. z 2006 r. Nr 156 poz. 1118 z późn. zm.) oraz § 11 ust. 1 pkt 1, § 15, § 24 ust. 1 rozporządzenia Ministra Transportu i Budownictwa z dnia 28 kwietnia 2006 r. w sprawie samodzielnych funkcji technicznych w budownictwie (Dz.U. Nr 86 poz. 578), Okręgowa Komisja Kwalifikacyjna Mazowieckiej Okręgowej Izby Inżynierów Budownictwa stwierdza, że:

Pan Piotr Maciej Wudarczyk

magister inżynier

urodzony dnia 8 lutego 1972 roku w Warszawie, syn Andrzeja

uzyskał

UPRAWNIENIA BUDOWLANE

nr MAZ/ 0424 /PWOE/06

**do projektowania i kierowania robotami budowlanymi bez ograniczeń
w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń
elektrycznych i elektroenergetycznych**

UZASADNIENIE

W związku z uwzględnieniem w całości żądania strony, na podstawie art. 107 § 4 Kodeksu postępowania administracyjnego odstępuje się od uzasadnienia decyzji.

Szczegółowy zakres nadanych uprawnień został opisany na odwrocie niniejszej decyzji

POUCZENIE

1. Zgodnie z art. 12 ust. 7 ustawy – Prawo budowlane, podstawę do wykonywania samodzielnych funkcji technicznych w budownictwie stanowi wpis do centralnego rejestru, prowadzonego przez Głównego Inspektora Nadzoru Budowlanego oraz wpis na listę członków właściwej izby samorządu zawodowego.

2. Od niniejszej decyzji służy odwołanie do Krajowej Komisji Kwalifikacyjnej Polskiej Izby Inżynierów Budownictwa w Warszawie za pośrednictwem Okręgowej Komisji Kwalifikacyjnej Mazowieckiej Okręgowej Izby Inżynierów Budownictwa w Warszawie, w terminie 14 dni od dnia jej doręczenia.

Skład Orzekający

1/ mgr inż. Krzysztof Latoszek

2/ mgr inż. Irena Churska

3/ mgr inż. Krzysztof Booss



Poświadczam
zgodność z oryginałem

Piotr Wudarczyk

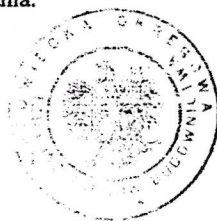
**Szczegółowy zakres uprawnień
do projektowania i kierowania robotami budowlanymi bez ograniczeń
w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń
elektrycznych i elektroenergetycznych**

I. Na mocy art. 12 ust. 1 pkt 1-5, art. 13 ust. 1, 3 i 4 ustawy - Prawo budowlane, w zakresie objętym wyżej wymienioną specjalnością, niniejsze uprawnienia stanowią podstawę do:

- 1/ projektowania, sprawdzania projektów architektoniczno-budowlanych i sprawowania nadzoru autorskiego,
- 2/ kierowania budową lub innymi robotami budowlanymi,
- 3/ kierowania wytwarzaniem konstrukcyjnych elementów budowlanych oraz nadzoru i kontroli technicznej wytwarzania tych elementów,
- 4/ wykonywania nadzoru inwestorskiego,
- 5/ sprawowania kontroli technicznej utrzymania obiektów budowlanych, z zastrzeżeniem art. 62 ust. 5.

II. Na mocy § 15 rozporządzenia Ministra Transportu i Budownictwa z dnia 28 kwietnia 2006 r. w sprawie samodzielnych funkcji technicznych w budownictwie, niniejsze uprawnienia budowlane stanowią podstawę do:
sporządzania projektu zagospodarowania działki lub terenu w zakresie wyżej wymienionej specjalności.

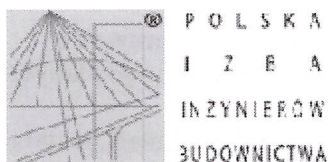
III. Na mocy § 24 ust. 1 rozporządzenia Ministra Transportu i Budownictwa z dnia 28 kwietnia 2006 r. w sprawie samodzielnych funkcji technicznych w budownictwie, niniejsze uprawnienia budowlane stanowią podstawę do:
projektowania obiektu budowlanego i kierowania robotami budowlanymi związanymi z obiektem budowlanym takim jak: sieci, instalacje i urządzenia elektryczne i elektroenergetyczne, w tym kolejowe, trolejbusowe i tramwajowe sieci trakcyjne wraz z urządzeniami do zasilania i sterowania.



Otrzymują:

1. Pan Piotr Maciej Wudarczyk
ul. Batuty 7 m. 1017
02-743 Warszawa
2. Główny Inspektor Nadzoru Budowlanego
3. a/a

Poświadczam
zgodność z oryginałem
Piotr Wudarczyk



Zaświadczenie

o numerze weryfikacyjnym:

MAZ-LW1-X18-QAA *

Pan PIOTR MACIEJ WUDARCZYK o numerze ewidencyjnym MAZ/IE/0120/07
adres zamieszkania ul. ELEKCYJNA 19 m. 33, 01-128 WARSZAWA
jest członkiem Mazowieckiej Okręgowej Izby Inżynierów Budownictwa i posiada wymagane
ubezpieczenie od odpowiedzialności cywilnej.
Niniejsze zaświadczenie jest ważne od 2019-02-01 do 2020-01-31.

Zaświadczenie zostało wygenerowane elektronicznie i opatrzone bezpiecznym podpisem elektronicznym
weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu w dniu 2018-11-14 roku przez:

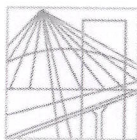
Roman Lulis, Przewodniczący Rady Mazowieckiej Okręgowej Izby Inżynierów Budownictwa.

(Zgodnie art. 9 ust 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. 2001 Nr 130 poz. 1430) dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi.)

* Weryfikację poprawności danych w niniejszym zaświadczeniu można sprawdzić za pomocą numeru weryfikacyjnego zaświadczenia na stronie Polskiej Izby Inżynierów Budownictwa www.piiib.org.pl lub kontaktując się z biurem właściwej Okręgowej Izby Inżynierów Budownictwa.

Proszę nie przysłać

Poświadczam
zgodność z oryginałem
Piotr Wudarczyk



WARMIŃSKO - MAZURSKA
OKRĘGOWA IZBA INŻYNIERÓW BUDOWNICTWA
OKRĘGOWA KOMISJA KWALIFIKACYJNA
 10-532 Olsztyn Plac Konsulatu Polskiego 1

WAM/OKK/U/125/05

Olsztyn, dnia 20 grudnia 2005 r.

D E C Y Z J A

Na podstawie art. 24 ust.1 pkt 2 ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów, inżynierów budownictwa oraz urbanistów /Dz.U. z 2001 r. Nr 5 poz. 42, ze zm.), art. 12 ust. 3, art.13 ust.1 pkt 1, art. 14 ust. 1 pkt 5 ustawy z dnia 07 lipca 1994 r. Prawo budowlane /tekst jednolity Dz.U. z 2003 r. Nr 207, poz. 2016 ze zm./, § 3 ust. 1, § 12 pkt 1 i § 24 ust. 1 rozporządzenia Ministra Infrastruktury z dnia 18 maja 2005 r. w sprawie samodzielnych funkcji technicznych w budownictwie /Dz.U. z 2005 r. Nr 96 poz. 817/ oraz art. 104 ust.1 i 2 Kodeksu postępowania administracyjnego /t.j. Dz.U. z 2000 r. Nr 98, poz.1071 ze zm./

**Okręgowa Komisja Kwalifikacyjna
 nadaje**

Panu MICHAŁOWI ANDRZEJOWI NIEDŹWIECKIEMU
 magistrowi inżynierowi elektrotechniki
 ur. 08 listopada 1970 r. w Nidzicy

UPRAWNIENIA BUDOWLANE

Nr ewid. WAM/0140/POOE/05

DO PROJEKTOWANIA BEZ OGRANICZEŃ

w specjalności instalacyjnej

w zakresie sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych

U Z A S A D N I E N I E

W związku z uwzględnieniem w całości żądania strony, na podstawie art. 107 § 4 K.p.a. odstępuje się od uzasadnienia decyzji. Zakres nadanych uprawnień budowlanych wskazano na odwrocie decyzji.

Pouczenie :

1. Zgodnie z art. 12 ust. 7 w/w ustawy Prawo budowlane – podstawę do wykonywania samodzielnych funkcji technicznych w budownictwie stanowi wpis, w drodze decyzji, do centralnego rejestru Głównego Inspektora Nadzoru Budowlanego oraz wpis na listę członków właściwej izby samorządu zawodowego, potwierdzony zaświadczeniem wydanym przez tę izbę, z określonym w nim terminem ważności.
2. Od decyzji niniejszej służy odwołanie do Krajowej Komisji Kwalifikacyjnej Polskiej Izby Inżynierów Budownictwa w Warszawie, za pośrednictwem Okręgowej Komisji Kwalifikacyjnej Warmińsko-Mazurskiej Okręgowej Izby Inżynierów Budownictwa w Olsztynie, w terminie czternastu dni od dnia jej doręczenia.



Skład orzekający OKK:

1. inż. Janusz Palmowski
2. mgr inż. Elżbieta Lasmanowicz
3. mgr inż. Sylwester Rączkiewicz

Poświadczam
 zgodność z oryginałem
 Michał Niedźwiecki

Pan Michał Andrzej Niedźwiecki upoważniony jest :

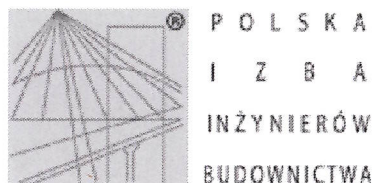
- I.** Na podstawie art.12 ust.1 pkt 1, art. 13 ust. 4 ustawy Prawo budowlane, w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych, bez ograniczeń do:
- a) projektowania, sprawdzania projektów architektoniczno-budowlanych i sprawowania nadzoru autorskiego,
 - b) sprawowania kontroli technicznej utrzymania obiektów budowlanych z zastrzeżeniem art.62 ust. 5 ustawy.
- II.** Na podstawie § 3 ust. 1 w/w rozporządzenia, uprawnienia budowlane do projektowania bez ograniczeń w odpowiedniej specjalności uprawniają do sporządzania projektu zagospodarowania działki lub terenu, w zakresie tej specjalności.
- III.** Na podstawie § 24 ust. 1 w/w rozporządzenia, uprawnienia niniejsze uprawniają do projektowania sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych, w tym kolejowych, trolejbusowych i tramwajowych sieci trakcyjnych wraz z urządzeniami do zasilania i sterowania.

Otrzymuje:

- 1. Pan Michał Andrzej Niedźwiecki
11-015 Olsztynek, Swaderki 12a
- 2. Okręgowa Rada Izby
- 3. Główny Inspektor Nadzoru Budowlanego
- 4. a/a

PRZEWODNICZĄCY
Okręgowej Komisji Kwalifikacyjnej
inż. Janusz Palmowski

Poświadczam
zgodność z oryginałem
Michał Niedźwiecki



Zaświadczenie

o numerze weryfikacyjnym:

WAM-WAZ-PAX-FE9 *

Pan Michał Niedźwiecki o numerze ewidencyjnym WAM/IE/0074/06
adres zamieszkania m. Swaderki 12a, 11-015 Olsztynek
jest członkiem Warmińsko-Mazurskiej Okręgowej Izby Inżynierów Budownictwa i posiada
wymagane ubezpieczenie od odpowiedzialności cywilnej.
Niniejsze zaświadczenie jest ważne do dnia 2020-03-31.

Zaświadczenie zostało wygenerowane elektronicznie i opatrzone bezpiecznym podpisem elektronicznym
weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu w dniu 2019-03-19 roku przez:

Mariusz Dobrzeński, Przewodniczący Rady Warmińsko-Mazurskiej Okręgowej Izby Inżynierów Budownictwa.

(Zgodnie art. 5 ust 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. 2001 Nr 130 poz. 1450) dane w postaci
elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są
równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi.)

* Weryfikację poprawności danych w niniejszym zaświadczeniu można sprawdzić za pomocą numeru weryfikacyjnego zaświadczenia na
stronie Polskiej Izby Inżynierów Budownictwa www.piib.org.pl lub kontaktując się z biurem właściwej Okręgowej Izby Inżynierów
Budownictwa.



Poświadczam
zgodność oryginałem
Michał Niedźwiecki
Michał Niedźwiecki

WARUNKI PRZYŁĄCZENIA



Orange Polska S.A.
Domena Hurt
Dostarczanie i Serwis Usług, Ewidencja i Standardy Infrastruktury
Dział Ewidencji i Zarządzania Danymi o Infrastrukturze
ul. Brzeska 24, 03-737 Warszawa
tel.: 22 664-60-89

PAS Projekt Sp. z o.o.
ul. Plantowa 5
05-830 Nadarzyn

Warszawa, 22 grudzień 2016 r.

Numer pisma: 85555/TODDRA/P/2015

Temat: techniczne warunki na przyłączenie do sieci telekomunikacyjnej budynku Biblioteki Narodowej przy Pl. Krasińskich 3/5 w Warszawie.

Szanowni Państwo,

W odpowiedzi na pismo z dnia 28.09.2016 roku oraz na podstawie załączonych planów, uprzejmie informujemy, że budynek Biblioteki Narodowej, zlokalizowany przy Pl. Krasińskich 3/5 w Warszawie, posiada przyłącze 1 otworowej kanalizacji teletechnicznej do sieci Orange Polska S.A. oraz ułożony w tej kanalizacji kabel rozdzielczy 10 parowy WA-D9C/30.

Z poważaniem

Wojciech Kobyliński
Starszy Specjalista ds. Zasobów Infrastruktury

Nadarzyn, 13.12.2019r.

Oświadczenie

Oświadczam, że projekt wykonawczy w zakresie branży elektrycznej i teletechnicznej dla projektu pn.:

**„Modernizacja energetyczna Pałacu Krasińskich (Pałacu Rzeczypospolitej)
przy Placu Krasińskich 3/5 w Warszawie”
z podziałem na etapy:**

Etap II – 2.3 – Modernizacja i aranżacja wnętrza Pałacu Krasińskich (Pałacu Rzeczypospolitej) przy Pałacu Krasińskich 3/5 w Warszawie”

został wykonany zgodnie z wymaganiami umowy, przepisami oraz zasadami wiedzy technicznej (art. 20 pkt. 4 ustawy z dnia 16 kwietnia 2004 roku o zmianie ustawy z 7 lipca 1994 roku – Prawo budowlane Dz. U. z dn. 9 lutego 2016 roku poz. 290), obowiązującymi przepisami techniczno – budowlanymi oraz obowiązującymi Polskimi Normami i stanowi kompletne opracowanie z punktu widzenia celu, któremu ma służyć.

mgr inż. Piotr Wudarczyk

Upewnienia budowlane do projektowania
i kierowania robotami budowlanymi
bez ograniczeń w specjalności instalacyjnej
w zakresie sieci, instalacji i urządzeń
elektrycznych i elektroenergetycznych
nr ewid. MAZ/0424/PWOE/06

PROJEKTANT

mgr inż. Piotr Wudarczyk

nr uprawnień: MAZ/0424/PWOE/06

mgr inż. Michał Niedźwiecki

Upewnienia budowlane do projektowania
bez ograniczeń w specjalności instalacyjnej
w zakresie sieci, instalacji i urządzeń
elektrycznych i elektroenergetycznych
nr ewid. WAM/0140/POOE/05

SPRAWDZAJĄCY

mgr inż. Michał Niedźwiecki

nr uprawnień: WAM/0140/POOE/05

PLAN BIOZ

Podstawą opracowania są następujące wytyczne:

Informacja dotycząca bezpieczeństwa i ochrony zdrowia (BIOZ)

Zgodnie z Rozporządzeniem Ministra Infrastruktury z dn.2002.06.23/Dz.U.NR 120poz. 1126/„W sprawie informacji dotyczącej bezpieczeństwa i ochrony zdrowia oraz planu bezpieczeństwa i ochrony zdrowia”, podaje się informacje, które winny być zawarte w „planie bioz”.

Informacja dotycząca bezpieczeństwa i ochrony zdrowia (BIOZ) – INFORMACJE OGÓLNE

Charakter robót budowlanych prowadzonych przy realizacji inwestycji stwarza ryzyko powstania zagrożenia bezpieczeństwa i zdrowia ludzi.

Przy prowadzeniu robót budowlanych należy:

- Wydzielić teren na którym prowadzone będą roboty przed dostępem osób postronnych.
- Oznakować miejsca prowadzenia prac.
- Urządzenia i instalacje energetyczne stwarzające zagrożenia dla zdrowia i życia ludzkiego należy zabezpieczyć przed dostępem osób nieupoważnionych.
- Miejsce przy urządzeniach energetycznych powinno być właściwie przygotowane, oznaczone i zabezpieczone w sposób określony w ogólnych przepisach bezpieczeństwa i higieny pracy.
- W każdym miejscu pracy, w którym wykonuje pracę zespół pracowników, powinien być wyznaczony kierujący tym zespołem.
- Wyłączenie urządzeń i instalacji elektroenergetycznych spod napięcia powinno być dokonane w taki sposób, aby uzyskać przerwę izolacyjną w obwodach zasilających urządzenia i instalacje.
- Prace w warunkach szczególnego zagrożenia dla zdrowia i życia ludzkiego, określone w ogólnych przepisach bezpieczeństwa i higieny pracy jako prace szczególnie niebezpieczne, powinny być wykonywane co najmniej przez dwie osoby, z wyjątkiem prac eksploatacyjnych z zakresu prób i pomiarów, konserwacji i napraw urządzeń i instalacji elektroenergetycznych o napięciu znamionowym do 1 kV, wykonywanych przez osobę wyznaczoną na stałe do tych prac w obecności pracownika asekurującego, przeszkolonego w udzielaniu pierwszej pomocy.
- Do robót używać sprzęt posiadający atesty. Stan techniczny narzędzi pracy i sprzętu ochronnego należy sprawdzać bezpośrednio przed jego użyciem. Narzędzia pracy i sprzęt ochronny, niesprawne lub które utraciły ważność próby okresowej, powinny być niezwłocznie wycofane z użycia.
- Prace pod napięciem należy wykonywać w oparciu o właściwą technologię pracy i przy zastosowaniu wymaganych narzędzi i środków ochronnych, określonych w instrukcji wykonywania tych prac.
- Przed przystąpieniem do wykonywania prac przy urządzeniach i instalacjach elektroenergetycznych wyłączonych spod napięcia należy:
 - o zastosować odpowiednie zabezpieczenie przed przypadkowym załączeniem napięcia,
 - o wywiesić tablicę ostrzegawczą w miejscu wyłączenia obwodu o treści: "Nie załączać",

- o sprawdzić brak napięcia w wyłączonym obwodzie,
- o uziemić wyłączone urządzenia,
- o zabezpieczyć i oznaczyć miejsce pracy odpowiednimi znakami i tablicami ostrzegawczymi.

- Prace rozruchowe, próby techniczne urządzeń i instalacji energetycznych powinny być prowadzone zgodnie z wymaganiami Polskich Norm, odrębnych przepisów, instrukcji eksploatacji oraz uzgodnione z ich użytkownikiem.
- Prace w warunkach szczególnego zagrożenia dla zdrowia i życia ludzkiego należy wykonywać na podstawie polecenia pisemnego, przy zastosowaniu odpowiednich środków zabezpieczających zdrowie i życie ludzkie.
- Zapewnić wykonawstwo robót przez pracowników posiadających aktualne badania lekarskie i wysokościowe oraz spełniający odpowiednie wymagania kwalifikacyjne dla rodzajów wykonywanych prac i zajmowanych stanowisk (zgodnie z Rozporządzeniem Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 28.04.2003r.
- Zapewnić nadzór nad budową przez osobę uprawnioną
- Zapewnić wszelkie wymagania z zakresu bezpieczeństwa i higieny pracy.

Informacja dotycząca bezpieczeństwa i ochrony zdrowia (BIOZ) – DOTYCZY INSTALACJI TELETECHNICZNYCH

1. Zakres robót i kolejność realizacji:

- demontaże istniejących instalacji teletechnicznych,
- montaż tras koryt i drabin kablowych,
- ułożenie instalacji teletechnicznych (w tym montaż kabli światłowodowych),
- montaż tablic i szaf teletechnicznych
- montaż osprzętu z podłączeniem,
- sprawdzenie instalacji teletechnicznej,
- pomiary instalacyjne,
- próby i uruchomienie instalacji.

2. Wykaz istniejących obiektów budowlanych w pasie prowadzonych robót

- w pasie prowadzonych robót występuje uzbrojenie budynku w instalacje: elektryczne, wodnokanalizacyjne, co oraz modernizowany budynek.

3. Elementy zagospodarowania mogące stwarzać zagrożenie bezpieczeństwa i zdrowia ludzi:

- niezabezpieczone przejścia,
- drabiny, rusztowania,
- pozostawione materiały i narzędzia,
- instalacje elektryczne placu budowy,
- spadające i występujące elementy w trakcie prowadzonych prac montażowych,
- praca w studniach kablowych
- wykopy
- montaż i obsługa kabli światłowodowych.

4. Przewidywane zagrożenia występujące podczas realizacji robót

Skala	Rodzaj zagrożenia	Miejsce	Czas występowania
-------	-------------------	---------	-------------------

Niska	potrącenie pojazdem mechanicznym	plac budowy	podczas wykonywania robót
Średnia	wpadnięcie do wykopu	wykopy pod sieci, uziemienie	podczas wykonywania robót
Średnia	przygnięcie	w miejscu załadunku, rozładunku i wykonania	podczas wykonania robót rozładunkowych i wykonywania instalacji
Średnia	upadek z wysokości	w budynku i na zewnątrz budynku	podczas wykonywania instalacji elektrycznych oraz inst. odgromowej
Średnia	natrafienie na wystające elementy	w budynku	od czasu rozpoczęcia prac do ich zakończenia
Średnia	porażenie prądem elektrycznym	w miejscu realizacji, prac, rozdzielnie elektryczne, wykonanie pomiarów elektrycznych	podczas wykonywania prac, pomiarów elektrycznych

5. Informacja o sposobie prowadzenia instruktażu pracowników:

- przed przystąpieniem do robót zapoznać pracowników z zakresem, charakterem i sposobem prowadzenia robót oraz o występujących zagrożeniach wynikających z projektu wykonawczego,
- pouczyć pracowników o sposobie zachowania się w przypadku wystąpienia zagrożeń,
- instruktaż stanowiskowy winien być odnotowany w zeszycie instruktaży,
- pracownicy w zakresie pełnionych obowiązków i posiadanej specjalizacji muszą posiadać zaświadczenia kwalifikacyjne i uprawnienia zawodowe.

6. Środki techniczne i organizacyjne zapobiegające niebezpieczeństwom wynikającym z wykonania robót w strefach szczególnego zagrożenia:

- wyposażyć pracowników w środki ochrony osobistej: rękawice, kaski i okulary ochronne,
- teren prowadzenia prac pod napięciem wygrodzić taśmą białą czerwoną, zawieszoną na wysokości 0,6-0,8m i tablicami ostrzegawczymi,
- wyposażenie pracowników w środki łączności.

7. Wskazanie miejsca przechowywania dokumentacji:

- projekt budowlany, dziennik, lista obecności oraz zeszyt instruktaż winny znajdować się w biurze budowy,
- pisemne polecenie na prace w pobliżu czynnych urządzeń elektroenergetycznych, winny być w posiadaniu brygadzysty.

JEDNOSTKA PROJEKTOWA

PAS PROJEKT Sp. z o.o.



ul. Plantowa 5;
05-830, Nadarzyn

TEL: (022) 739-90-25, FAX: (022) 739-79-06

www.pasprojekt.com

NAZWA INWESTYCJI / BUDOWY

"Modernizacja i aranżacja wnętrz Pałacu Krasińskich
(Pałacu Rzeczypospolitej) przy Placu Krasińskich 3/5 w
Warszawie"

FAZA OPRACOWANIA

nr kat.

etap projektu

120.3

PROJEKT WYKONAWCZY

TOM I ROZDZIAŁ 4 PROJEKT INSTALACJI TELETECHNICZNYCH

CZĘŚĆ GRAFICZNA

ADRES INWESTYCJI / BUDOWY

pl. Krasińskich 3/5 00-207
Warszawa

NR EWIDENCYJNY DZIAŁKI

dz. nr ew. 4, obręb 5-02-07, j. ewidencyjna Warszawa-Śródmieście

INWESTOR :

Biblioteka Narodowa
al. Niepodległości 213, 02-086 Warszawa

mgr inż. Piotr Włodarczyk

Uprawnienia budowlane do projektowania
i kierowania robotami budowlanymi
bez ograniczeń w specjalności instalacyjnej
w zakresie sieci, instalacji i urządzeń
elektrycznych i elektroenergetycznych
nr ewid. M/227/424/PWOE/06

mgr inż. Michał Niedźwiecki

Uprawnienia budowlane do projektowania
bez ograniczeń w specjalności instalacyjnej
w zakresie sieci, instalacji i urządzeń
elektrycznych i elektroenergetycznych
nr ewid. WAM/0140/PWOE/05

DATA OPRACOWANIA

REW. Z 10-2019 r. DO PROJEKTU Z 04-2017 r.