

Spis treści

1.	DANE OGÓLNE	3
1.1.	Przedmiot opracowania	3
1.2.	Inwestor	3
1.3.	Wykonawca dokumentacji	3
1.4.	Adres budowy	3
1.5.	Zakres opracowania	3
1.6.	Warunki ogólne	3
1.7.	Wykonawca robót	3
1.8.	Uwagi dotyczące przyjętych rozwiązań sprzętowych	4
2.	Trasy kablowe, zasilanie instalacji teletechnicznych	4
2.1.	Założenia projektowe	4
2.2.	Trasy kablowe	4
2.2.1.	Montaż tras kablowych	4
2.2.2.	Rozprowadzenie instalacji teletechnicznych	4
3.	Sieć strukturalna	4
3.1.	Normy i zalecenia	4
3.2.	Założenia projektowe	5
3.3.	Zakres opracowania	5
3.4.	Wymagania ogólne dotyczące systemu okablowania strukturalnego	5
3.5.	Wymagania ogólne dotyczące wykonawcy systemu okablowania strukturalnego	5
3.6.	Opis projektowanego systemu	5
3.6.1.	Okablowanie poziome	6
3.6.2.	Punkty przyłączeniowe użytkowników	6
3.6.3.	Panele rozdzielcze RJ45 19"	6
3.6.4.	Skretkowe kable instalacyjne	6
3.6.5.	Kable krosowe RJ45	6
3.6.6.	Kable przyłączeniowe RJ45	6
3.6.7.	Punkty dystrybucyjne	6
3.6.8.	Okablowanie szkieletowe	6
3.6.9.	Kable instalacyjne światłowodowe	6
3.6.10.	Panele rozdzielcze światłowodowe 19"	7
3.6.11.	Kable krosowe światłowodowe	7
3.7.	Montaż instalacji strukturalnej	7
3.7.1.	Punkty logiczne PL	7
3.7.2.	Okablowanie poziome miedziane	7
3.7.3.	Okablowanie pionowe- szkieletowe	7
3.7.3.1.	<i>Okablowanie światłowodowe</i>	7
3.7.3.2.	<i>Łączność telefoniczna- okablowanie miedziane</i>	8
3.7.4.	System numeracji gniazd, przyłączy i okablowania	8
3.8.	Pomiary i testy	8
3.8.1.	Pomiary kabli miedzianych	8
3.8.2.	Pomiary kabli światłowodowych	8
3.8.3.	Wyniki pomiarów	9
3.9.	Zalecenia i szczegółowe wymagania instalacyjne	9
3.10.	Zalecenia eksploatacyjne	9
3.11.	Centrala telefoniczna	9
3.12.	Aktywne urządzenia komputerowe	9
4.	Kontrola dostępu	10
4.1.	Normy i zalecenia	10
4.2.	Założenia projektowe	10
4.3.	System kontroli dostępu KD	10
4.3.1.	Charakterystyka systemu KD	10
4.3.2.	Instalacja i montaż systemu KD	10
4.3.3.	Montaż	10
4.3.4.	Uruchamianie i oprogramowanie systemu	11
4.3.5.	Warunki odbioru i protokół odbiorowy	11
4.3.6.	Eksploatacja i konserwacja	11
4.3.7.	Protokół Odbiorowy	11
4.4.	System wideodomofonowy	11
4.4.1.	Dobór systemów	11
4.4.2.	Opis systemów	12
4.4.3.	Montaż elementów systemu wideodomofonowego	12
4.4.3.1.	<i>Montaż paneli wideodomofonowych</i>	12
4.4.3.2.	<i>Montaż wideomonitorów</i>	12
4.4.3.3.	<i>Okablowanie systemu</i>	12
4.4.3.4.	<i>Uruchomienie i Oprogramowanie systemu</i>	12
4.5.	Eksploatacja i konserwacja	12
5.	Telewizja naziemna RTV	12
5.1.	Założenia projektowe	12
5.2.	Zakres opracowania	12
5.3.	Budowa sieci telewizyjnej	12
5.3.1.	Punkt dystrybucyjny	12
5.3.2.	Trasy kablowe	12
5.3.3.	Uziemienie systemu i ochrona galwaniczna	12
5.3.4.	Gniazda końcowe	13
5.4.	Pomiary	13
6.	Telewizja dozorowa CCTV	13
6.1.	Struktura systemu	13

6.2.	Montaż kamer.....	13
6.3.	Okablowanie systemu.....	13
6.4.	Punkt dystrybucyjny wydzielonej sieci strukturalnej telewizji dozorowej	13
6.5.	Zasilanie kamer	13
6.6.	Rejestracja i podgląd obrazu	13
6.7.	Pomiary i testy.....	14
6.7.1.	Pomiary	14
6.7.2.	Testy	14
6.8.	Eksploatacja i konserwacja.....	14
7.	System przywoławczy.....	14
7.1.	Normy dotyczące systemów przywoławczych.....	14
7.2.	Założenia projektowe.....	14
7.3.	Sposób prowadzenia okablowania systemowego	14
7.4.	Zasilanie systemu.....	15
7.5.	Oprogramowanie systemu.....	15
7.6.	Pomiary.....	15
7.7.	Testy.....	15
8.	Zintegrowany System Bezpieczeństwa.....	15
8.1.	Ogólne założenia dla systemu	15
8.2.	System Zarządzania Bezpieczeństwem PSIM – zasada działania	16
8.3.	Opis funkcjonalny systemu	16
8.4.	Struktura systemu (Opracowanie aplikacji graficznej)	16
8.5.	Urządzenie integrujące wraz z oprogramowaniem – Moduł integratora.....	18
8.6.	Część graficzna i tekstowa (opracowanie układu graficznego aplikacji	18
8.7.	Nawigacja obiektowa, czyli wprowadzenie układu graficznego i planów akcji.....	18
8.8.	Procedury (Wprowadzenie procedur działań i akcji).....	19
8.9.	Zdarzenia alarmowe (konfiguracja filtrów i priorytetów alarmów).....	19
8.10.	Moduł analizująco-raportujący	19
8.11.	SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM BUDYNKU	19
8.12.	Wymagania systemu zarządzania bezpieczeństwem.....	19
8.13.	Możliwości integracyjne.....	20
8.14.	Integracja z systemem sygnalizacji pożaru	21
8.15.	Integracja z Systemem Nadzoru Wizyjnego CCTV	22
8.16.	Integracja z Systemem Włamania i Napadu.....	22
8.17.	Integracja z Dźwiękowym Systemem Ostrzegawczym	23
8.18.	Integracja z systemem gazów medycznych	23
8.19.	Moduł Powiadomiania SMS	23
8.20.	Moduł MOBILE PSIM.....	23
8.21.	Integracja z opcjonalnymi systemami bezpieczeństwa.....	23
9.	Uwagi końcowe	24
10.	Tabele.....	24
11.	Rysunki	24

1. DANE OGÓLNE

1.1. Przedmiot opracowania

Przedmiotem opracowania niniejszego projektu wykonawczego jest uszczegółowienie projektu technicznego instalacji teletechnicznych w projektowanych oddziałach Budyńku Głównego Szpitala Klinicznego im. K. Jonschera Uniwersytetu Medycznego im. K. Marcinkowskiego w Poznaniu.

1.2. Inwestor

Szpital Kliniczny im. K. Jonschera Uniwersytetu Medycznego
im. K. Marcinkowskiego w Poznaniu,
ul. Szpitalna 27/33, 60-572 Poznań

1.3. Wykonawca dokumentacji

A.DO XXI
Spółka z ograniczoną odpowiedzialnością
Ul. Trybunalska 38, 60-325 Poznań
tel. 061 862 1234, fax: 061 8

1.4. Adres budowy

ul. Szpitalna 27/33, 60-572 Poznań

1.5. Zakres opracowania

Projekt przewiduje budowę i montaż następujących instalacji teletechnicznych :

- Sieć strukturalna
- Kontrola Dostępu
- Telewizja RTV
- Telewizja dozorowa CCTV
- System przywoławczy

UWAGA:

Niniejszy projekt został opracowany przy wykorzystaniu urządzeń, systemów, wyposażenia konkretnych firm wskazanych w dokumentacji. Wskazanie producentów miało na celu zapewnienie wysokiego standardu wykonania projektowanych instalacji a nie promocje producentów. Dlatego projektant nie wyklucza zastosowanie innych urządzeń innych konkurencyjnych firm jednakże o parametrach nie gorszych od zastosowanych w projekcie.

Projektowany oddział jest częścią istniejącego kompleksu szpitalnego. W związku z powyższym zastosowane urządzenia teletechniczne muszą być zgodne i kompatybilne z istniejącymi urządzeniami teletechnicznymi. Nie dopuszcza się systemów, które nie będą umożliwiały integracji z istniejącymi urządzeniami

1.6. Warunki ogólne

Wykonawca jest zobowiązany do zapoznania się z kompletną specyfikacją projektową obiektu i dokonaniem koordynacji montażowych niniejszej instalacji z innymi instalacjami mechanicznymi i elektrycznymi. Wszelkie zmiany montażowe wynikające z braku koordynacji wykonania w/w instalacji z innymi branżami Wykonawca ma zrealizować na własny koszt.

Specyfikacje, opisy i rysunki uwzględniają oczekiwany przez Inwestora standard dla materiałów, urządzeń i instalacji. Wykonawca może zaproponować rozwiązanie alternatywne niemniej jednak w takim przypadku musi uzyskać pisemne zatwierdzenie Inwestora. Rysunki i część opisowa są w dokumentacji wzajemnie uzupełniającymi się. Wszystkie elementy ujęte w części opisowej a nie pokazane na rysunkach oraz pokazane na rysunkach a nie ujęte w specyfikacji winny być traktowane jakby były ujęte w obu. W przypadku wątpliwości co do interpretacji niniejszej dokumentacji, Wykonawca przed złożeniem oferty powinien ją wyjaśnić z Inwestorem oraz uzasadnionych przypadkach z Projektantem.

Wszystkie wykonywane prace oraz proponowane materiały winny odpowiadać Polskim Normom i posiadać stosowne deklaracje zgodności lub posiadać znak CE. Do zakresu prac Wykonawcy każdorazowo wchodzi próby urządzeń i instalacji wg. obowiązujących norm i przepisów oraz protokolarny odbiór w obecności Inwestora. Do wykonanych prac Wykonawca winien załączyć również deklaracje kompletności wykonanych prac oraz zgodności z projektem i niniejszą dokumentacją.

1.7. Wykonawca robót

Zgodnie z obowiązującymi przepisami wykonawca robót instalacji teleinformatycznych i teletechnicznych zostanie wyłoniony w drodze przetargu z przedsiębiorstw branży budownictwa telekomunikacyjnego i teletechnicznego. Wykonawca winien wystąpić o zezwolenie na prowadzenie robót od Inwestora oraz uzyskać niezbędne pozwolenie wynikające z obowiązującego prawa budowlanego i ustaleń zawartych w uzgodnieniach branżowych.

Wymaga się, aby Kierownik Robót posiadał uprawnienia w specjalności telekomunikacyjnej bez ograniczeń wydane po 2006 roku wystawione minimum dwa lata przed datą składania oferty, oraz aktualne zaświadczenie przynależności do Okręgowej Izby Inżynierów Budownictwa

Wykonawca musi posiadać co najmniej 1 osobę posiadającą Certyfikat Instalatora danego systemu wydanego przez Producenta systemu mającego siedzibę na terenie Polski.

Wykonawca powinien posiadać świadectwo kwalifikacyjne SEP dozorowe i eksploatacyjne.

1.8. Uwagi dotyczące przyjętych rozwiązań sprzętowych

Wszystkie podane w niniejszej dokumentacji nazwy i typy wraz z nazwami producentów urządzeń i materiałów zostały przyjęte w celu określenia ich parametrów technicznych i standardów i należy traktować je jako przykładowe - ze względu na zasady ustawy Prawo Zamówień Publicznych, a zwłaszcza art. 29 do 31. Wynika z niego prawo projektanta do skróconego podania charakterystyk technicznych poprzez podanie symbolu handlowego, co wcale nie oznacza konkretnego producenta wyrobu. Dopuszcza się możliwość zastosowania rozwiązań równoważnych do proponowanych w projekcie wykonawczym pod warunkiem zachowania standardów jakościowych i sprzętowych. Proponowane rozwiązania techniczne zostały przyjęte aby były podstawą wykonania rzetelnego kosztorysu i oferty. W przypadku zmiany elementów systemu lub całego systemu należy zwrócić uwagę na kompatybilność elementów i założenia działania systemów.

Zgodnie z Ustawą Prawo Zamówień Publicznych Projektant dopuszcza zastosowanie urządzeń i materiałów spełniających inne równoważne normy niż te wskazane w Projekcie.

Użyte w projekcie określenie „lub równoważne” oznacza równoważność zgodnie z Ustawą Prawo Zamówień Publicznych z dnia 11.09.2019 z późniejszymi zmianami.

2. Trasy kablowe, zasilanie instalacji teletechnicznych

2.1. Założenia projektowe

W celu rozprowadzenia instalacji teletechnicznych należy zaprojektować system przepustów i tras kablowych.

2.2. Trasy kablowe

2.2.1. Montaż tras kablowych

W celu rozprowadzenia instalacji teletechnicznej po obiekcie zaprojektowano trasy kablowe. Projekt przewiduje montaż metalowych koryt kablowych siatkowych serii KDS na głównych trasach kablowych. Koryta kablowe o szerokości 100mm i 200mm należy instalować pod sufitem właściwym w przestrzeni międzysufitowej. W większości tras kablowych korytka należy montować na zawieszach ściennych o odpowiedniej długości. W przypadku braku możliwości zamontowania zawieszów ściennych należy stosować wsporniki sufitowe z zawieszami. Koryta kablowe należy montować w przestrzeni międzysufitowej 10cm nad sufitem podwieszanym. Sposób skrzyżowań należy ustalić indywidualnie na etapie wykonawstwa. Wszystkie metalowe elementy tras kablowych należy uziemić.

2.2.2. Rozprowadzenie instalacji teletechnicznych

Kable należy prowadzić w zaprojektowanych korytach kablowych, kanałach, przepustach kablowych, rurkach elektroinstalacyjnych i pod tynkiem. W związku z dużą różnorodnością kabli instalacji teletechnicznych i przesyłanych sygnałów możliwy jest niekorzystne oddziaływanie w/w kabli na siebie. Przenikające się pola elektromagnetyczne mogą wprowadzać np. błędy - zakłócenia w transmisjach sygnału. W związku z powyższym należy pamiętać o grupowaniu kabli jednego systemu w pęczki przy pomocy opasek zaciskowych. **UWAGA: Do spinania kabli instalacji strukturalnej należy stosować taśmy montażowe. Ma to zapobiec deformacji wiązki kablowej co ma wpływ na parametry transmisyjne okablowania.** Kable w korytach powinny być układane równoległe do siebie, a liczba skrzyżowań powinna być jak najmniejsza. Na całej trasie kablowej nie należy dopuszczać do nadmiernych naprężeń i skręceń na kablach oraz należy zachować normatywne promienie gięcia. W celu łatwiejszej identyfikacji kabli instalacji teletechnicznych na obiekcie kable powinny być oznakowane przy pomocy tabliczek znaczeniowych (naklejek) z dwóch stron kabla. Na tabliczkach powinny znaleźć się informacje o typie kabla, relacji, rodzaju instalacji i danych wykonawcy. W przypadku prowadzenia kabli poza projektowanymi korytami należy je zabezpieczyć np., za pomocą rurek elektroinstalacyjnych RL.

Uwaga: Wszystkie kable sygnałowe i zasilające nowe i modernizowane prowadzone w pomieszczeniach i w częściach użytkowych – widocznych bezwzględnie muszą być układane pod tynkiem.

3. Sieć strukturalna

3.1. Normy i zalecenia

- PN-EN 50173-1: aktualne Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne i strefy biurowe;
- PN-EN 50174-1: aktualne Technika informatyczna. Instalacja okablowania
- Część 1: Specyfikacja i zapewnienie jakości;
- PN-EN 50174-2: aktualne Technika informatyczna. Instalacja okablowania.
- Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków;
- BN-84/8984-10 Zakładowe sieci telekomunikacyjne wewnętrzne. Instalacje wewnętrzne
- normy zakładowe TP S.A.

3.2. Założenia projektowe

Na terenie projektowanego oddziału należy zaprojektować nowoczesną sieć teleinformatyczną. Projektowana sieć powinna posiadać topologię gwiazdy. Sieć powinna zapewnić technologię dla pełnego wykorzystania aplikacji (dzisiaj i w przyszłości) oraz pozwalać na łatwą zmianę konfiguracji poszczególnych gniazd. Pomiędzy nowym punktem dystrybucyjnym, a przełącznicą światłowodową w piwnicy należy ułożyć okablowanie światłowodowe 12J. Pomiędzy nowym punktem dystrybucyjnym, a przyłączem telefonicznym w hallu obiektu należy ułożyć okablowanie telefoniczne kablem YTKSY 25x2x0,5.

W budynku szpitala należy zaprojektować nowoczesną sieć strukturalną kategorii 6a F/UTP.

3.3. Zakres opracowania

Zakres opracowania obejmuje:

- Instalację okablowania strukturalnego
- Montaż okablowania poziomego
- Ułożenie i zakończenie w węzłach sieci okablowania szkieletowego światłowodowego i miedzianego telefonicznego

3.4. Wymagania ogólne dotyczące systemu okablowania strukturalnego

System okablowania strukturalnego ma zapewnić niezawodną i wydajną warstwę fizyczną sieci teleinformatycznej, która zagwarantuje wystarczający zapas parametrów transmisyjnych dla działania dzisiejszych i przyszłych aplikacji transmisyjnych. W celu spełnienia najwyższych wymogów jakościowych i wydajnościowych należy zapewnić:

- Okablowanie miedziane kategorii 6.a
- Okablowanie skrętkowe w wersji ekranowanej.
- Okablowanie światłowodowe jednomodowe.
- Wszystkie produkty muszą być fabrycznie nowe.
- Celem idealnego dopasowania komponentów, wszystkie produkty okablowania muszą pochodzić od jednego producenta i być oznaczone jego nazwą lub logo.
- Producent okablowania strukturalnego musi spełniać wymagania międzynarodowej normy odnośnie standardów jakości ISO 9001, należy przedłożyć odpowiedni certyfikat.
- Producent okablowania musi objąć zainstalowany system bezpłatną, 25-letnią systemową gwarancją niezawodności, która obejmie tory transmisyjne miedziane i światłowodowe w zakresie łącza Channel (kable instalacyjne, panele 19", złącza, kable krosowe i przyłączeniowe). Gwarancja musi być trójstronną umową podpisaną pomiędzy Użytkownikiem, Wykonawcą okablowania oraz Producentem.
- Producent okablowania jest zobligowany do reasekuracji zobowiązań gwarancyjnych Wykonawcy, w przypadku niemożności wywiązania się Wykonawcy z tych zobowiązań. Reasekuracja obejmuje okres, na jaki została udzielona gwarancja.
- Warunkiem udzielenia systemowej gwarancji niezawodności jest wykonanie instalacji zgodnie z obowiązującymi normami okablowania strukturalnego oraz zgodnie z zaleceniami producenta. Instalacja musi być wykonana przez Certyfikowanego Instalatora systemu okablowania.

3.5. Wymagania ogólne dotyczące wykonawcy systemu okablowania strukturalnego

Celem profesjonalnego wykonania instalacji okablowania strukturalnego, na najwyższym poziomie jakości i wydajności, wszystkich czynności instalacyjnych musi dokonać wykwalifikowana firma spełniająca poniższe wymagania:

- Firma wykonawcza musi zatrudniać pracowników – Certyfikowanych Instalatorów posiadających ważne uprawnienia i certyfikat wydany przez producenta okablowania przyjętego w tym projekcie.
- Certyfikat Instalatora musi być wydany po odbyciu szkolenia, w którym każdy Instalator zdobędzie wszystkie niezbędne umiejętności praktyczne i teoretyczne, uprawniające do instalowania, serwisowania, tworzenia dokumentacji powykonawczej oraz wykonywania pomiarów certyfikacyjnych sieci.
- Certyfikat Instalatora, który posiadają osoby wykonujące instalację musi być dokumentem terminowym wydawanym na okres jednego roku. Po tym czasie instalator musi go przedłużyć na kolejny rok, uczestnicząc w szkoleniu realizowanym przez producenta lub dystrybutora okablowania.
- Wykonawca autoryzujący system okablowania strukturalnego musi posiadać uprawnienia do objęcia zainstalowanego systemu 25-letnią systemową gwarancją niezawodności.

3.6. Opis projektowanego systemu

Sieć strukturalna kategorii 6a projektowana w obiekcie szpitalnym będzie miała topologię gwiazdy, co zapewni możliwość szybkich zmian w strukturze okablowania oraz łatwą lokalizację i usuwanie usterek. W przypadku uszkodzenia dowolnej linii, przestaje pracować tylko ta stacja robocza – (telefon, komputer), która jest podłączona poprzez uszkodzoną linię. Na obiektach projektuje się instalację strukturalną, w skład której wchodzić będzie okablowanie poziome i okablowanie pionowe.

Dokładną lokalizację punktów logicznych przedstawiono na załączonych rzutach architektonicznych. Okablowanie poziome sieci strukturalnej wykonane zostanie kablem miedzianym typu F/UTP kategorii 6a. Kable zakończone zostaną w punktach logicznych na modułach RJ45. Okablowanie pionowe wykonane zostanie za pomocą wieloparowych kabli miedzianych komputerowych i telekomunikacyjnych oraz kabli światłowodowych OTK jednomodowych.

3.6.1. Okablowanie poziome

Zadaniem okablowania poziomego jest zapewnienie wydajnej i niezawodnej transmisji danych pomiędzy punktami dystrybucyjnymi, a punktami przyłączeniowymi użytkowników. Długość kabla instalacyjnego, pomiędzy gniazdem RJ45 w panelu rozdzielczym a gniazdem przyłączeniowym użytkownika (nie licząc kabli krosowych i przyłączeniowych) nie powinna przekraczać 90m. Celem zapewnienia wysokiej wydajności należy zastosować okablowanie co najmniej klasy Ea (kategorii 6a) wg najnowszych aktualnych standardów okablowania strukturalnego ISO/IEC 11801:2011 (który zastępuje normy ISO/IEC 11801:2002, ISO/IEC 11801 AMD1:2006, ISO/IEC 11801 AMD2:2010), EN 50173-1:2011, TIA-568-C.2. Zagwarantuje to odpowiedni zapas parametrów transmisyjnych dla zapewnienia transmisji danych Ethernet 10Gb/s zgodnie ze standardem IEEE 802.3an. Zgodność z powyższymi normami należy udokumentować certyfikatami wydanymi przez laboratorium badawcze Delta, w zakresie całego łącza oraz niezależnych komponentów (kabel, panel, złącze RJ45).

Celem zapewnienia zasilania urządzeniom końcowym, należy zastosować komponenty okablowania strukturalnego zapewniające przesył energii zgodnie ze standardem PoEP (ang. Power over Ethernet Plus) wg IEEE 802.3at o mocy do 30W.

3.6.2. Punkty przyłączeniowe użytkowników

Gniazda przyłączeniowe użytkowników (Punkty Logiczne – PL) należy zorganizować w postaci 1 lub 2 modułów RJ45 keystone montowanych w adapterze z tworzywa sztucznego o wymiarach 45x45 mm. Ten uniwersalny standard montażowy zapewni organizację gniazd użytkowników w zależności od potrzeb, w formie natynkowej, podtynkowej lub w kasetach podłogowych w oparciu o osprzęt elektroinstalacyjny wielu producentów, również w połączeniu z gniazdami zasilania 230V, celem stworzenia punktów elektryczno logicznych (tzw. PEL).

3.6.3. Panele rozdzielcze RJ45 19"

Przeznaczeniem paneli rozdzielczych RJ45 19" jest zakończenie skrętkowych kabli instalacyjnych, które zbiegają się do punktu dystrybucyjnego z powierzchni obiektu obsługiwanych przez dany punkt dystrybucyjny. Następnie łącza okablowania z panela rozdzielczego łączone są, przy użyciu kabli krosowych, z portami RJ45 urządzeń aktywnych lub z portami centrali telefonicznej.

3.6.4. Skrętkowe kable instalacyjne

W celu implementacji wydajnych aplikacji, w okablowaniu poziomym przewidziano zastosowanie kabli skrętkowych 4-pary F/UTP kat.6a

3.6.5. Kable krosowe RJ45

Zadaniem kabli krosowych RJ45 jest połączenie łącza okablowania poziomego zakończonych na panelu rozdzielczym z portami RJ45 urządzeń aktywnych lub z portami centrali telefonicznej.

3.6.6. Kable przyłączeniowe RJ45

Zadaniem kabli przyłączeniowych RJ45 jest dołączenie urządzeń końcowych (komputerów, telefonów IP, punktów itd.) do gniazd przyłączeniowych – punktów logicznych rozmieszczonych w obiekcie.

3.6.7. Punkty dystrybucyjne

Przewiduje się montaż nowego punktu dystrybucyjnego. Punkty dystrybucyjne będą się składać z szaf teletechnicznych 19" wiszącej o wielkości 42U wyposażone w panele rozdzielcze miedziane i światłowodowe, panele porządkowe, panel zasilający i UPS.

3.6.8. Okablowanie szkieletowe

Rolą okablowania szkieletowego jest zapewnienie połączeń pomiędzy głównym a pośrednimi punktami dystrybucyjnymi. Ta część okablowania strukturalnego jest bardzo ważna z punktu widzenia wydajności i niezawodności systemu, ponieważ zapewnia wymianę danych pomiędzy węzłowymi punktami sieci oraz agregację ruchu danych od wielu użytkowników sieci w tym samym czasie. Dlatego okablowanie szkieletowe należy wykonać z odpowiednim zapasem parametrów transmisyjnych oraz zapasem ilości łączy, w celu uniknięcia nadmiernych obciążeń (wąskich gardeł) w systemie.

3.6.9. Kable instalacyjne światłowodowe

W połączeniach szkieletowych, pomiędzy głównym a pośrednimi punktami dystrybucyjnymi, należy zastosować kable światłowodowe spełniające poniższe wymagania:

- Pojemność 12 włókien
- Włókna jednomodowe SM
- Konstrukcja kabla typu U-DQ(ZN)BH, uniwersalna z możliwością układania wewnątrz budynku i na zewnątrz budynku (w rurach osłonowych).
- Wzmocniona konstrukcja w postaci luźnej centralnej tuby, wypełnionej żelem chroniącym przed wilgocią oraz zmniejszającym tarcie pomiędzy włóknami w czasie układania.
- Konstrukcja kabla musi zawierać wzmocnienie w postaci włókien szklanych, które dodatkowo muszą zapewniać ochronę antygrzyzoniową.
- W celu spełnienia wymogów przeciwpożarowych należy zastosować kabel w powłoce zewnętrznej LSZH (ang. Low Smoke Zero Halogen), czyli wykonanej z materiału bezhalogenowego emitującego ograniczoną ilość szkodliwych substancji w czasie pożaru.
- Wymagane parametry kabla światłowodowego

Parametr	Wartość
Średnica zewnętrzna kabla (maksymalna)	7 mm
Waga kabla (maksymalna)	50 kg/km
Siła ciągnięcia (maksymalna)	1600 N
Promień gięcia (minimalny)	104 mm
Odporność na zginięcie(maksymalna)	1500 N/dm
Zakres temperatury instalacji	-5 /+50 °C

3.6.10. Panele rozdzielcze światłowodowe 19”

Kable światłowodowe w szafach 19” należy zakańczać w światłowodowych panelach rozdzielczych, 19” 1U ze złączami SC/APC duplex. Włókna należy zakończyć w technologii spawania (pigtaile należy dobrać zgodnie z typem włókna w kablu instalacyjnym). Należy zastosować panele spełniające poniższe wymogi:

- Pojemność do 48 włókien, dzięki czemu otrzymamy dużą efektywność rozmieszczenia włókien na 1U.
- Łatwy dostęp do wnętrza poprzez wysuwaną szufladę.
- Konstrukcja wykonana z metalu z ochronnym pokryciem antykorozyjnym.
- 4 otwory w ścianie tylnej do wprowadzenia kabli instalacyjnych za pośrednictwem przepustów kablowych PG.
- W podstawie panela na wysokości przepustów PG muszą znajdować się elementy pozwalające na zamocowanie trwale do szuflady przełącznicy kabla instalacyjnego, zapobiegając przed przypadkowym wysunięciem się kabla.
- Standardowo panel w komplecie musi zawierać:
 - 4 uchwyty do organizacji włókien,
 - opaski zaciskowe,
 - śruby do montażu w stelażu 19”,
 - przepusty PG oraz zaślepki pod niewykorzystane porty PG,
 - gniazda przepustowe (ilość zależna od pojemności zakańczonego kabla),
 - pigtaile (ilość zależna od pojemności zakańczonego kabla),
 - kasety, uchwyty oraz osłony na spawy dla zabezpieczenia spawów światłowodowych.

3.6.11. Kable krosowe światłowodowe

Zadaniem kabli krosowych światłowodowych jest połączenie łączy okablowania szkieletowego, zakończonych na panelu rozdzielczym z portami światłowodowymi urządzeń aktywnych. Należy zastosować kable krosowe spełniające poniższe wymogi:

- Złącza SC z obydwu stron kabla.
- Konstrukcja 2-włóknowa duplex, celem zapewnienia 2-kierunkowej transmisji Ethernet.
- Rodzaj włókien tego samego typu jak w kablu instalacyjnym.
- Szybka i łatwa lokalizacja połączeń w punkcie dystrybucyjnym dzięki świetlnej identyfikacji połączeń.
- Długość należy dostosować do odległości pomiędzy panelem światłowodowym a urządzeniami aktywnymi.

3.7. Montaż instalacji strukturalnej

3.7.1. Punkty logiczne PL

Punkty logiczne należy wykonać w standardzie RJ45 kat 6a, jako gniazda pojedyncze i podwójne montowane natynkowo lub podtynkowo. Na załączonych rysunkach przedstawiono przybliżoną lokalizację montażu gniazd instalacji strukturalnej.

W pomieszczeniach biurowych-medycznych punkty logiczne należy instalować w puszkach podtynkowych o głębokości 6,0 cm. Wysokość montażu punktów logicznych proponuje się na wysokości stołu. Dokładną lokalizację oraz wysokość montażu gniazd strukturalnych należy określić na etapie wykonawstwa uwzględniając lokalizację montażu gniazd elektrycznych i aranżację pomieszczeń. Do budowy punktów logicznych należy wykorzystać gniazda RJ45 keystone.

3.7.2. Okablowanie poziome miedziane

W celu implementacji wydajnych aplikacji, w okablowaniu poziomym przewidziano zastosowanie kabli skrętkowych ekranowanych typu F/UTP kat.6a w powłoce zewnętrznej LSZH. W projekcie przewiduje się układanie kabli w trasach kablowych instalacji teletechnicznych. Podejścia do gniazd należy wykonać podtynkowo w przygotowanych wcześniej bruzdach kablowych, kanałach, listwach i przepustach kablowych. Przy układaniu kabli instalacji strukturalnej należy zwrócić szczególną uwagę na odległość kabli od instalacji elektrycznych i oświetlenia jarzeniowego.

Kable instalacji poziomej na panelach i od strony punktu logicznego należy rozszyć na modułach RJ45 kategorii 6a Keystone.

3.7.3. Okablowanie pionowe- szkieletowe

Rolą okablowania szkieletowego jest zapewnienie połączeń pomiędzy głównym a pośrednimi punktami dystrybucyjnymi. Ta część okablowania strukturalnego jest bardzo ważna z punktu widzenia wydajności i niezawodności systemu, ponieważ zapewnia wymianę danych pomiędzy węzłowymi punktami sieci oraz agregację ruchu danych od wielu użytkowników sieci w tym samym czasie. Dlatego okablowanie szkieletowe należy wykonać z odpowiednim zapasem parametrów transmisyjnych oraz zapasem ilości łączy, w celu uniknięcia nadmiernych obciążeń (wąskich gardeł) w systemie. Dlatego okablowanie szkieletowe należy wykonać przy użyciu dwóch typów mediów transmisyjnych:

- Kabel światłowodowy jednomodowego
- Wieloparowy kabel telefoniczny dla połączeń telefonii analogowej i cyfrowej

3.7.3.1. Okablowanie światłowodowe

W celu budowy połączenia pionowego nowego punktu dystrybucyjnego z główną serwerownią szpitala przewiduje się montaż łączy światłowodowego. Kable światłowodowe OTK 12J należy prowadzić pomiędzy poszczególnymi PD a serwerownią główną w piwnicy

budynku. Dodatkowo należy ułożyć kabel OTK 48J pomiędzy projektowaną serwerownią, a istniejącą serwerownią w budynku bloków operacyjnych. Kable należy prowadzić w trasach kablowych instalacji teletechnicznych. Przy układaniu kabla światłowodowego należy zwrócić szczególną uwagę na sposób układania kabli światłowodowych, trzeba zachować normatywny promień gięcia oraz nie dopuścić do nadmiernego ucisku na kabel, co może spowodować mikropęknięcia na włóknach światłowodowych. W szafach teletechnicznych należy pozostawić zapas kabla OTK o długości około 10,0m każdy. W projektowanych punktach dystrybucyjnych kable światłowodowe należy rozszyc na przełącznicy światłowodowej wyposażonej w podwójne gniazda typu SC/APC. Włókna światłowodowe należy zakończyć wtykami pigtailami SC. Łączenie pigtaili należy wykonać przez spawanie włókien.

3.7.3.2. Łączność telefoniczna- okablowanie miedziane

W celu rozprowadzenia sygnału telefonicznego i zapewnienia pełnego zakresu usług telefonicznych w obiekcie, do punktu dystrybucyjnego przewiduje się ułożenie kabla typu YTKSY 25x2x0,5. Kabel ten należy ułożyć pomiędzy projektowanymi punktami dystrybucyjnymi PD a szafą GPDT. Kable należy prowadzić w istniejących trasach i przepustach kablowych. Kable w punkcie dystrybucyjnym należy zakończyć na panelu krosowych RJ 45 kat. 3. Dodatkowo należy ułożyć 4 kable YKSY 53x2x0,5 pomiędzy szafą GPDT a centralą telefoniczną. Kabel należy prowadzić w piwnicy budynku.

3.7.4. System numeracji gniazd, przyłączy i okablowania

Wszystkie gniazda oznaczyć należy szyldami z opisem wykorzystując do tego celu jednolity system numeracji przedstawiony poniżej:
PD1/12

Gdzie: Szafa/numer gniazda

Uwagi:

- Każdy punkt logiczny musi być indywidualnie oznaczony unikatowym numerem
- Dla danego łącza numeracja musi być identyczna po stronie punktu logicznego i panela rozdzielczego
- Kable w szafie teletechnicznej muszą być jednoznacznie oznaczone zgodnie z przyjętą nomenklaturą. Oznaczenie kabli należy wykonać przy panelu rozdzielczym.

Projektant nie wyklucza innego oznakowania gniazd logicznych, jednakże konieczna jest wtedy akceptacja Inwestora.

3.8. Pomiary i testy

Po wykonaniu instalacji okablowania strukturalnego wykonawca musi przeprowadzić odpowiednie pomiary sprawdzające (certyfikacyjne), wszystkich łączy miedzianych skrętkowych i światłowodowych, potwierdzające, iż wykonane okablowanie strukturalne spełnia wymagania norm. Pomiary należy przeprowadzić zgodnie z wartościami granicznymi zdefiniowanymi w ISO 11801 lub EN 50173. Wyniki wszystkich pomiarów muszą być pozytywne. Pomiary należy wykonać przyrządem w pełni sprawnym, posiadającym ważny certyfikat potwierdzający przejście procesu kalibracji u producenta, co będzie potwierdzeniem poprawności jego wskazań. Do dokumentacji powykonawczej należy dołączyć wymieniony certyfikat kalibracji oraz raport z wynikami pomiarów wszystkich łączy okablowania skrętkowego i światłowodowego.

3.8.1. Pomiary kabli miedzianych

Wszystkie łączy skrętkowe w systemie należy przetestować pod kątem spełniania wymogów kategorii 6a wg ISO 11801 lub EN 50173:

- Należy przeprowadzić pomiary w układzie pomiarowym typu „Channel” (łącznie z kablami krosowymi i kablami przyłączeniowymi). Do pomiaru każdego łącza należy użyć odrębnej pary kabli połączeniowych, która w przyszłości powinna być wykorzystywana w powiązaniu właśnie z tym łączem. W związku z powyższym należy zapewnić pełen zestaw kabli połączeniowych RJ45.
- Pomiary należy wykonać miernikiem o poziomie dokładności, co najmniej „Level IV”. Zalecane typy mierników: DTX-1800 lub DTX-1200 firmy Fluke Networks.
- Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łącza, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania.
- Wyniki pomiarów certyfikacyjnych wszystkich łączy muszą być prawidłowe.
- Pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346.
- Wymagany zakres mierzonych parametrów dla każdej z par (kombinacji par):
 - Mapa połączeń - poprawność i ciągłość wykonanych połączeń
 - Straty odbiciowe (ang. RL - Return Loss)
 - Straty wtarceniowe - tłumienie (ang. IL - Insertion Loss)
 - Straty przesłuchów zbliżonych (ang. NEXT - Near End Crosstalk Loss)
 - Sumaryczny parametr NEXT (ang. PSNEXT – Power Sum NEXT)
 - Współczynnik tłumienia w odniesieniu do straty przesłuchu na bliskim końcu (ang. ACR-N – Attenuation to Crosstalk Ratio at the Near end)
 - Sumaryczny współczynnik ACR-N (ang. PSACR-N – Power Sum ACR-N)
 - Współczynnik tłumienia w odniesieniu do straty przesłuchu na dalekim końcu (ang. ACR-F – Attenuation to Crosstalk Ratio at the Far end)
 - Sumaryczny współczynnik ACR-F (ang. PSACR-F – Power Sum ACR-F)
 - Rezystancja pętli dla prądu stałego (ang. DC current loop)
 - Opóźnienie propagacji (ang. Propagation delay)
 - Różnica opóźnień propagacji (ang. Delay skew)

Dla telekomunikacyjnych kabli rozdzielczych należy przeprowadzić pomiary:

1. prądem stałym
2. pomiar tłumienności skutecznej przy jednej częstotliwości

3.8.2. Pomiary kabli światłowodowych

Wszystkie łącza światłowodowe w systemie należy przetestować pod kątem spełniania wymogów norm ISO-11801 lub EN-50173:

- Należy przeprowadzić pomiary dwukierunkowe, w których źródło świetlnego sygnału referencyjnego będzie umieszczone w pierwszym kroku na jednym końcu łącza, a w kolejnym kroku na drugim końcu łącza.
- Łącza jednomodowe (SM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 1310 nm i 1550 nm.
- Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łącza, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania.
- Wyniki pomiarów certyfikacyjnych wszystkich łączy musza być prawidłowe.
- Pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346.
- Wymagany zakres mierzonych parametrów:
 - Ciągłość łącza.
 - Długość łącza.
 - Tłumienie włókien dla dwóch długości fali.

3.8.3. Wyniki pomiarów

Wyniki pomiarów dla kabli miedzianych i światłowodowych w formie wydruku jak i w wersji elektronicznej musza być dołączone do dokumentacji powykonawczej.

Dokumentacja powykonawcza musi zawierać:

- plany instalacji oraz schematów połączeń okablowania pionowego - miedzianego i światłowodowego,
- plany instalacji oraz schematów połączeń okablowania poziomego
- opis rozszycia kabli miedzianych na panelach krosowniczych, panelach telefonicznych i PG
- schemat połączenia włókien światłowodowych
- pomiary okablowania pionowego i poziomego (miedzianego i światłowodowego)
- karty katalogowe, certyfikaty, instrukcje DTR wykorzystanych urządzeń.

Dokumentację powykonawczą wraz z wynikami pomiarów należy dostarczyć w wersji elektronicznej oraz w dwóch egzemplarzach drukowanych.

3.9. Zalecenia i szczegółowe wymagania instalacyjne

Instalację okablowania strukturalnego należy wykonać z najwyższą starannością z zachowaniem wytycznych znajdujących się w normach okablowania strukturalnego oraz wytycznych producenta okablowania. Szczególnie należy zastosować się do:

- Instalator musi zwrócić szczególną uwagę, by nie naruszyć struktury kabli podczas montażu. Należy przestrzegać bezpiecznych promieni gięcia kabli skrętkowych i światłowodowych, sił naciągu, sił zgniatających oraz przestrzegać zakresu temperatur w czasie instalacji. Dopuszczalne zakresy wymienionych parametrów można znaleźć w specyfikacjach technicznych produktów.
- Kable skrętkowe należy montować w złączach RJ45 zachowując minimalny rozplot par wprowadzanych do złącza.
- Długość skrętkowych kabli instalacyjnych pomiędzy gniazdami RJ45 w panelu rozdzielczym a gniazdami przyłączeniowymi nie może być większa niż 90m.
- Każdy moduł powinien posiadać możliwość rozszycia kabla według schematu T568A i T568B. Zaleca się stosowanie rozszycia wg schematu T568B.
- Wszystkie metalowe części szaf i stelaży dystrybucyjnych musza zostać uziemione.
- W celu ochrony przed niepożądanym dostępem wszystkie szafy dystrybucyjne oraz pomieszczenia teletechniczne powinny zostać wyposażone w drzwi z zamkami zabezpieczającymi.
- Instalując okablowanie skrętkowe należy zachowywać poniższe bezpieczne odległości od kabli zasilających:

Typ kabla	Odległość od instalacji zasilającej [mm]		
	Brak przegrody metalicznej	Przegroda metalowa perforowana	Przegroda metalowa pełna
Kable F/FTP	10	5	0
Kable U/FTP; F/UTP	50	25	0
Kabel UTP	100	50	0

- Tabela obowiązuje dla wiązki 15 obwodów 230V / 20A. W przypadku mniejszej ilości obwodów, odległości proporcjonalnie się zmniejszają.
- Kable 3-fazowe należy traktować, jako 3 kable 1-fazowe.
- Obwody o prądzie większym niż 20A należy traktować, jako proporcjonalna wielokrotność obwodów 20A.
- Powyższe zalecenia obowiązuja w przypadku prawidłowego uziemienia ekranów kabli transmisyjnych i metalicznych elementów tras kablowych.

3.10. Zalecenia eksploatacyjne

Wszelkie zmiany wynikłe podczas eksploatacji systemu (zmiana połączeń, krosowań połączeń światłowodowych) należy niezwłocznie korygować w oznacznikach systemu i wprowadzać do dokumentacji.

3.11. Centrala telefoniczna

Zgodnie z ustaleniami z Inwestorem niniejszy projekt nie obejmuje dostawy, rozbudowy, modernizacji centrali telefonicznej.

3.12. Aktywne urządzenia komputerowe

W modernizowanych pomieszczeniach szpitala klinicznego projektuje się montaż przełączników komputerowych 48 portowe RJ45 warstwy 2 z i bez zasilania PoE. Połączenia między przełącznikami będą wykonane za pomocą łączy światłowodowych z wykorzystaniem modułów światłowodowych SFP. Przełączniki komputerowe należy zainstalować w szafach teletechnicznych poszczególnych punktów dystrybucyjnych i podłączyć do zasilania 230V. Ponadto zostanie zamontowany punkt dostępowy łączności bezprzewodowej WiFi.

W serwerowni planuje się montaż urządzeń aktywnych i serwerów w celu stworzenia zapasowej przestrzeni obsługi szpitala. Dobór elementów został pokazany w zestawieniu materiałów.

Podłączenie punktów logicznych do przełącznika należy wykonać zgodnie z numeracją uwzględniającą rozmieszczenie punktów logicznych na obiekcie. Standardem w obiekcie szpitalnym są urządzenia HP ARUBA.

4. Kontrola dostępu

4.1. Normy i zalecenia

- Ustawa o Ochronie Osób i Mienia z dnia 22 sierpnia 1997, Dz. U. 97.114.740,
- Rozporządzenie MSWiA w sprawie szczególnych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne, Dz. U. 98.129.858,
- PN-EN 50133-1:2007 - Systemy alarmowe -- Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia -- Część 1: Wymagania systemowe
- PN-EN 50133-2-1:2002 - Systemy alarmowe -- Systemy kontroli dostępu stosowane w zabezpieczeniach -- Część 2-1: Wymagania dla podzespołów
- PN-EN 50133-7:2002 - Systemy alarmowe -- Systemy kontroli dostępu stosowane w zabezpieczeniach -- Część 7: Zasady stosowania
- Materiały szkoleniowe Centrum Szkolenia przy Polskiej Izbie Systemów Alarmowych
- BN-84 8984-10 Zakładowe sieci telekomunikacyjne przewodowe instalacje wewnętrzne
- BN-84/8984-10- Instalacje wewnętrzne. Ogólne wymagania.
- BN-73/9371-03- Uziemienie urządzeń telekomunikacji przewodowej i bezprzewodowej. Ogólne wymagania i badania.
- Zalecenia producentów urządzeń
- Ustawa z dnia 7 lipca 1994 r. "Prawo Budowlane" (j.t.: Dz.U. 2000 Nr109 poz.1126 ze zm.),
- Rozporządzenie Ministra Infrastruktury w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie z dnia 12 kwietnia 2002r, i późniejsze nowelizacje,

4.2. Założenia projektowe

W nowoprojektowanych pomieszczeniach szpitala klinicznego należy zamontować nowoczesny system kontroli dostępu KD i instalacji domofonowej, obejmującym wyznaczone przez Inwestora wejścia do oddziałów pooperacyjnych.

4.3. System kontroli dostępu KD

4.3.1. Charakterystyka systemu KD

W szpitalu klinicznym istnieje system kontroli dostępu KD oparty o kontrolery dostępu serii PR402 firmy Roger. Kontroler ten obsługuje pojedyncze przejścia KD. Odblokowanie drzwi następuje po zbliżeniu uprawnionej karty do głowicy czytającej. System umożliwia nadawanie w prosty sposób uprawnień do przejścia przez odpowiednie drzwi. Podczas pracy obiektu wszystkie przejścia kontroli dostępu są udostępniane według zaprogramowanych reguł na podstawie weryfikacji kart zbliżeniowych przypisanych poszczególnym osobom.

Każde przejście kontroli dostępu wyposażone jest w przycisk ewakuacyjny. Jego użycie spowoduje bezwarunkowe odłączenie zasilania elektromechanicznych elementów blokujących zainstalowanych na danym przejściu. Użycie tego przycisku pozostawia trwały ślad w okolicach przycisku (stłuczona lub wgnieciona szybka).

4.3.2. Instalacja i montaż systemu KD

Projekt zakłada montaż kontrolerów PR402 w zestawie z zasilaczem tzw. wersja SET. Drzwi objęte kontrolą dostępu należy wyposażyć w mechaniczne elementy blokujące i monitorujące stan zamknięcia.

Do zasilania central przewidziano obwodów 230V AC z rozdzielnic elektrycznych. Punkt zasilające znajdują się na załączonych rzutach architektonicznych. Instalację 230V wykonano przewodem YDY 3x1,5mm² 750V.

Wszystkie czujniki i elementy wykonawcze systemu zasilane są napięciem stałym stabilizowanym 12V pochodzącym z zasilacza umieszczonego w obudowach kontrolerów.

Kable i przewody prowadzić należy w zależności od aranżacji pod tynkowo do urządzeń. Do prowadzenia kabli i przewodów w pierwszej kolejności należy korzystać z głównych tras kablowych.

Sterowniki systemu ROGER dostarczone w obudowie z zestykiem antysabotażowym montować w pomieszczeniach chronionych na wysokości zapewniającej swobodny dostęp serwisowy. Przyciski i czytniki zbliżeniowe montować w miejscach zapewniających estetyczny wygląd i funkcjonalność.

4.3.3. Montaż

Montaż przeprowadzić z uwzględnieniem poniższych uwag:

- Do realizacji systemu przewidziano przewody teletechniczne typu LiYY 8x0,75, typu OMY 2x0,5, typu UTP4x2x0,5 i YTDY
- Kable instalacji systemu KD prowadzić podtynkowo, w rurkach plastikowych. Główne trasy kablowe ułożyć w korytach kablowych. Sposób montażu i prowadzenia ciągów kablowych jest przedstawiony na planach tras kablowych w części rysunkowej.

- W okolicy każdego z przejść KD zainstalować puszkę rozdzielczą tak, aby do centrali KD zbiegało się jak najmniej pojedynczych przewodów. Puszki te zamontować natynkowo w miejscu zapewniającym minimalizację długości przewodów połączeniowych, w sposób nie szpecący pomieszczenia, ale zapewniający w późniejszym czasie dostęp serwisowy. W miejscach gdzie zaprojektowano sufity podwieszane przewidzieć otwory rewizyjne, aby możliwy był dostęp serwisowy.
- Czytniki KD montować na specjalnych podstawkach dystansowych natynkowo.
- Centrale KD montować w miejscach wskazanych w dokumentacji na wysokości umożliwiającej dostęp serwisowy.
- Ze względu na występujące uzbrojenie (kable, inne przeszkody) Wykonawca może wnieść zmiany w sposobie prowadzenia instalacji, po uprzednim uzyskaniu zgody Projektanta oraz Inwestora. Po uzyskaniu akceptacji należy sporządzić Protokół Uzgodnień na okoliczność zmian.
- Zwrócić szczególną uwagę na montaż czujników magnetycznych, aby ich elementy były spasowane osiowo na danym przejściu.
- Każdy kabel wprowadzany do puszkę lub innych urządzeń musi być jednoznacznie oznakowany - numerowany zgodnie z projektem – posiadać symbol urządzenia docelowego. Napis powinien być wykonany flamastrem wodoodpornym na całej szerokości kabla i umieszczony 15 cm przed jego zakończeniami.
- Należy zapewnić odpowiedni zapas kabla (około 1m) przy elemencie docelowym.
- Czytniki kart magnetycznych jak i zielony przycisk ewakuacyjny należy na wysokości około 1,5m. Drzwi przejść KD wyposażać należy w kontaktrony magnetyczne jako czujniki stanu drzwi, elektrorygły jako elementy utrzymujące drzwi w stanie zamkniętym i samozamykacze.
- Jako elementy ryglujące stosować elektrorygły typu rewersyjnego o konstrukcji panicznej – EFFEFF serii 332 bez monitoringu
- W sterowniku kable należy rozszyć na odpowiednich portach zwracając szczególną uwagę na odpowiednia polaryzację czytników KD.
- Projektowane sterowniki KD należy sieciować ze sobą i wpiąć w moduł ethernetowy UT-4

4.3.4. Uruchamianie i oprogramowanie systemu

Po wykonaniu wszystkich połączeń należy przystąpić do włączenia, programowania i uruchomienia systemu. Włączenie zasilania systemu musi odbywać się zgodnie z zaleceniami producenta centrali.

Przed programowaniem centrali należy szczegółowo uzgodnić z użytkownikiem systemu dane wyjściowe do programowania centrali (nazwy stref, nazwy partycji, nazwę systemu, imiona i nazwiska użytkowników, ich uprawnienia do obsługi systemu). Oprogramowanie systemu kontroli dostępu należy wykonać zgodnie z przejętym podziałem na przejścia kontroli dostępu.

4.3.5. Warunki odbioru i protokół odbiorowy.

Podczas odbioru należy:

- Sprawdzić kompletność instalacji zgodnie z dokumentacją wykonawczą bądź powykonawczą (jeżeli jest sporządzona),
- Sprawdzić kompletność elementów zgodnie z dokumentacją wykonawczą bądź powykonawczą (jeżeli jest sporządzona),
- Sprawdzić oznakowanie elementów KD,
- Dokonać pomiarów rezystancji izolacji przewodów,
- Sprawdzić poprawność wykonania i działania systemu,

Wykonawca pozostawi inwestorowi następującą dokumentację:

- uaktualniony projekt wykonawczy bądź powykonawczy (jeżeli jest sporządzony),
- protokoły pomiarów rezystancji izolacji i uziemienia,
- Protokół pozytywnego testu systemu.

4.3.6. Eksploatacja i konserwacja

Niezawodność działania systemu uwarunkowana jest zachowaniem właściwych warunków pracy, napięcia zasilania, stanem akumulatorów oraz przeprowadzeniem badań okresowych.

Badania okresowe powinny być przeprowadzane przez Zakład Serwisowy, któremu użytkownik zlecił konserwację instalacji. Zaistniałe uszkodzenia powinny być bezzwłocznie zgłaszane Serwisowi.

4.3.7. Protokół Odbiorowy

Po przeprowadzeniu odbioru zostanie przekazany protokół odbiorowy, który będzie zawierał:

- datę i miejsce przeprowadzenia próby,
- nazwę Zleceniodawcy i wykaz osób działających z jego ramienia wraz z zajmowanymi stanowiskami,
- nazwę systemu,
- rodzaj i wynik przeprowadzonych prób,
- stwierdzenie, czy urządzenie jest wykonane zgodnie z projektem wykonawczym (jeżeli istnieje konieczność wykonania dokumentacji powykonawczej należy ją niezwłocznie przedłożyć do inwestora i dokonać ponownego odbioru wraz z nowym Protokołem Odbioru),
- wnioski komisji odbiorowej,
- podpisy wraz z pieczętkami osób upoważnionych.

Po dokonaniu odbioru urządzenia, powyższy protokół należy włączyć do założonej Książki Eksploatacji Systemu.

4.4. System wideodomofonowy

4.4.1. Dobór systemów

Projekt przewiduje wyposażenie obiektu w instalacje wideodomofonową cyfrową w technologii IP.

4.4.2. Opis systemów

W projektowanym obiekcie przewiduje się montaż paneli wideodomofonowych przy wejściach do pomieszczeń szpitalnych. Dokładną lokalizację projektowanych urządzeń przedstawiają załączone rzuty architektoniczne. W rejestracji planuje się montaż wideomonitora.

4.4.3. Montaż elementów systemu wideodomofonowego

4.4.3.1. Montaż paneli wideodomofonowych

Na obiekcie proponuje się montaż paneli. Lokalizację montażu urządzeń przedstawiają załączone plany. Montaż paneli w obiekcie przewiduje się na wysokości 1,5m nad posadzką. Dokładną lokalizację montażu paneli należy ustalić na etapie wykonawstwa, w miejscu łatwo dostępnym uwzględniającym aranżację i wystrój budynku. Zasilanie paneli domofonowych należy wykonać w technologii PoE.

4.4.3.2. Montaż wideomonitorów

Na obiekcie planuje się montaż wideomonitora w pomieszczeniu rejestracji. Zasilanie wideomonitora należy wykonać w technologii PoE.

4.4.3.3. Okablowanie systemu

Połączenia kablowe pokazano na schemacie.

4.4.3.4. Uruchomienie i Oprogramowanie systemu

Uruchomienie i oprogramowanie systemu wideodomofonowego należy wykonać zgodnie z dokumentacją DTR.

4.5. Eksploatacja i konserwacja

Niezawodność działania systemu uwarunkowana jest zachowaniem właściwych warunków pracy, napięcia zasilania, stanem akumulatorów oraz przeprowadzeniem badań okresowych. Badania okresowe powinny być przeprowadzane przez Zakład Serwisowy, któremu użytkownik zlecił konserwację instalacji. Zaistniałe uszkodzenia powinny być bezzwłocznie zgłaszane Serwisowi.

5. Telewizja naziemna RTV

5.1. Założenia projektowe

W budynku przewiduje się przebudowę i rozbudowę sieci telewizyjnej naziemnej rozdzielczej umożliwiającej niezależny odbiór lokalnych programów radiowych i telewizyjnych.

5.2. Zakres opracowania

Zakres rzeczowy niniejszego opracowania obejmuje demontaż istniejącego wzmacniacza, demontaż okablowania antenowego, demontaż anten, montaż nowych anten, montaż szafki, instalację wzmacniaczy, gniazd RTV i okablowanie abonenckiego. Szczegóły instalacji zostały pokazane na rysunkach.

5.3. Budowa sieci telewizyjnej

5.3.1. Punkt dystrybucyjny

Przewiduje się przebudowę istniejącego punktu dystrybucyjnego, aby umożliwić rozbudowę instalacji. Szczegóły rozbudowy zostały pokazane na rysunku.

5.3.2. Trasy kablowe

Kable wizyjne typu RG6 od punktu dystrybucyjnego do gniazd RTV należy prowadzić w projektowanych trasach kablowych i rurkach elektroinstalacyjnych.

5.3.3. Uziemienie systemu i ochrona galwaniczna

Wszystkie elementy układu należy uziemić $R < 10\Omega$. W szczególności należy zwrócić uwagę na uziemienie układów aktywnych i pasywnych całego systemu.

5.3.4. Gniazda końcowe

Zgodnie z projektem instalacji telewizji kablowej, niniejsza dokumentacja wskazuje miejsce montażu gniazd RTV. Dokładną lokalizację montażu gniazd należy ustalić na etapie wykonawstwa uwzględniając aranżację wnętrza oraz montaż gniazd elektrycznych 230V.

5.4. Pomiary

Po wybudowaniu instalacji telewizji kablowej należy przeprowadzić właściwe pomiary. Wymagania odnośnie poszczególnych parametrów można znaleźć w opracowaniu: „Wymagania Techniczne i Eksploatacyjne dla Antenowych Instalacji Zbiorowych Przeznaczonych Do Reemisji Usług Radiodifuzji Naziemnej” wydanej przez Grupę ds. techniki i sprzętu Międzyresortowego Zespołu ds. Telewizji i Radiofonii Cyfrowej.

6. Telewizja dozorowa CCTV

Zadaniem Systemu Telewizji Dozorowej jest obserwacja i kontrolowanie chronionych stref w celu ewentualnego zapobieżenia nieprzewidzianym sytuacjom oraz odpowiednie szybkie reagowanie w przypadku zaistnienia aktów bezprawnej ingerencji (kradzież, napad, rozbój). Zadaniem tego systemu jest uzupełnienie funkcjonowania pozostałych systemów bezpieczeństwa (KD, SAP). Dodatkowo system CCTV instalowany w salach operacyjnych szpitala klinicznego ma za zadanie monitorować stan pacjentów i zakres wykonywanych czynności przez personel medyczny przy pacjentach.

6.1. Struktura systemu

Projekt zakłada montaż systemu CCTV IP oparty o kolorowe kamery wysokiej rozdzielczości. Okablowanie systemu zostanie zaprojektowane w topologii gwiazdy. Sygnał z kamer kodowany protokołem IP transmitowany będzie poprzez wydzieloną sieć LAN do serwera wizyjnych.

6.2. Montaż kamer

Kamery należy zamontować w miejscach wskazanych na rzutach architektonicznych. W budynku kamery należy montować na suficie podwieszanym.

6.3. Okablowanie systemu

Zgodnie z założeniami kamery systemu telewizji dozorowej mają działać w technologii IP i być zasilane po skrętce komputerowej w systemie PoE. W związku z powyższym na terenie obiektu zakłada się budowę wydzielonej sieci instalacji strukturalnej. Do punktu dystrybucyjnego schodzić się będzie okablowanie ze wszystkich kamer telewizji dozorowej. Ze względu na niewielkie odległości punktu dystrybucyjnego od kamer nie przekraczającego 90,0 m okablowanie kamer CCTV zostanie wykonane w technologii kabla skrętkowego, zgodnie z przyjętym standardem na obiekcie.

6.4. Punkt dystrybucyjny wydzielonej sieci strukturalnej telewizji dozorowej

Punkt dystrybucyjny wydzielonej sieci strukturalnej należy umieścić w projektowanej szafie teletechnicznej 19". Szafę należy doposażyć w panele rozdzielcze, zasilające, prowadnice kabli, przełącznik komputerowy PoE. Sposób montażu punktu dostępowego został ujęty w projekcie instalacji strukturalnej

6.5. Zasilanie kamer

Projekt zakłada zasilanie kamer telewizji dozorowej w oparciu o standard PoE IEEE 802.3af.

6.6. Rejestracja i podgląd obrazu

Obraz ze wszystkich kamer telewizji dozorowej archiwizowany zostanie na 2 serwerach wizyjnych zlokalizowanych w serwerowni w piwnicy budynku szpitala klinicznego. W związku z rozbudową systemu monitoringu wizyjnego istniejący system należy rozbudować o dodatkowe 2 serwery wyposażone w pełni w dyski 10 TB. Należy także dostarczyć oprogramowanie do zarządzania rozbudowanym systemem (oprogramowanie musi umożliwiać zarządzanie wieloma serwerami). Należy także zapewnić 128 licencji dla kanałów wideo IP.

Wymagania serwera systemu telewizji dozorowej:

Serwer do pracy w trybie ciągłym, o solidnej konstrukcji, bazujący na obudowie przemysłowej RACK 19" 4U wykonanej z blachy stalowej 1mm. Zalecany do systemów wymagających bardzo długiego okresu archiwizacji nagrań. **Obsługujący kamery sieciowe zgodne ze standardami ONVIF, PSIA, RTSP. W zestawieniu materiałów wskazano modele referencyjne urządzeń.**

6.7. Pomiary i testy

6.7.1. Pomiary

W związku z budową okablowania wizyjnego i zasilającego na bazie sieci strukturalnej pomiary tej sieci należy wykonać zgodnie z wytycznymi ujętymi w dokumentacji instalacji strukturalnej

6.7.2. Testy

Po wykonaniu instalacji należy wykonać następujące testy:

1. Test poprawności wykonania połączeń.
2. Test poprawności wykonania okablowania.
3. Test pracy systemu w poszczególnych strefach.

6.8. Eksploatacja i konserwacja

Niezawodność działania systemu uwarunkowana jest zachowaniem właściwych warunków pracy, napięcia zasilania, oraz przeprowadzeniem badań okresowych. Badania okresowe powinny być przeprowadzane przez Zakład Serwisowy, któremu użytkownik zlecił konserwację instalacji. Zaistniałe uszkodzenia powinny być bezzwłocznie zgłaszane Serwisowi.

7. System przywoławczy

7.1. Normy dotyczące systemów przywoławczych

Podstawową normą obowiązującą w Europie jest norma EN 793 określająca wyposażenie i standaryzację obiektów szpitalnych. Współgra z nią norma DIN 0834 określająca sposób działania systemów szpitalnych; przywoławczych, alarmowych czy p-poż. oraz obostrzenia z tym związane.

DIN 0834 obowiązuje od 2005 roku i zastąpiła starą normę DIN 41085.

Część 1 normy DIN 0834 dotycząca systemów przywoławczych stosowanych w szpitalach określa następujące wymogi :

- a. systemy przywoławcze muszą być podłączone do UPS-ów zapewniających zasilanie przez okres co najmniej 1-2 godzin po zaniku napięcia.
- b. systemy powinny posiadać możliwość rejestracji zdarzeń / drukarka lub komputer /.
- c. powierzchnia przycisku nie mniejsza niż 1cm² – przywołanie musi być potwierdzone optycznie
- d. magistrale systemowe nie mogą być wykorzystywane do innych celów.
- e. sygnalizacja wezwania musi nastąpić nie później niż po 5-sekundach.
- f. jednoznaczne oznakowanie elementów inne od reszty elementów.
- g. wielkość elementów sygnalizacyjnych, rozpoznawanie kolorów z odległości co najmniej 30 metrów, widoczność lamp i sygnalizatorów pod kątem 180-stopni.
- h. kolory użyte w sygnalizacji wezwań systemowych to:
- i. czerwony-wezwania pielęgniarские i alarmowe z sygnalizacją akustyczną do powiadamiania personelu.
- j. Żółty/biały -wezwania z toalet i łazienek,
- k. zielony-zaznaczanie/ potwierdzenie / obecności personelu pielęgniarского – system musi rozpoznawać gdzie się znajduje personel, związane to jest z przekazywaniem przywołań
- l. wymagane jest przekazanie akustyczne / może być dodatkowo optyczne /.
- m. możliwość przywołań dodatkowych lub alarmów technicznych.
- n. sygnalizacja wyjęcia przycisku gruszkowego z gniazda.
- o. autokontrola systemu / testowanie wewnętrzne wykrywanie uszkodzeń elementów oraz ciągłości przewodów /.
- p. określone zostają również wysokości montażu elementów systemu;
- q. przyciski przywoławcze i kasowniki na wysokości od 0,7 do 1,5 metra,
- r. przyciski z wyświetlaczem 1,5 –1,8 metra, centralki na wysokości 1,6 – 1,8 metra,
- s. lampki sygnalizacyjne oraz wyświetlacze na wysokości od 1,5 do 2,2 metra,
- t. w toaletach ciągną przycisku sznurkowego nie może znajdować się wyżej niż 30cm nad podłogą.
- u. zakaz odwoływania wezwań z centrali systemu !!!
- v. aby zapobiegać przypadkowemu skasowaniu wezwania z toalety znajdującej się w sali chorych nakazuje się umieszczenie dodatkowego kasownika w samej toalecie.

Zgodnie z dyrektywą niskich napięć instalacja powinna przebiegać w odległości min.30cm od instalacji 230V, na odległościach mniejszych niż 10 metrów w odległości nie mniejszej niż 10cm.

7.2. Założenia projektowe

W rozbudowywanym oddziale należy zainstalować system przywoławczy w pokojach pacjentów i toaletach dla osób niepełnosprawnych. System będzie się składał z przycisków pociągowych, manipulatorów przy łóżkach, przycisku kasującego, zasilacza, lampki sygnalizacyjnej nad drzwiami oraz wyświetlacza w rejestracji i pokoju lekarzy.

7.3. Sposób prowadzenia okablowania systemowego

Okablowanie zasilająco sterujące systemu należy prowadzić po trasach instalacji teletechnicznych. Połączenia urządzeń systemu przywoławczego należy wykonać zgodnie z załączonym schematem i dokumentacją DTR

7.4. Zasilanie systemu

System przywoławczy zasilany jest napięciem 24V. W obiekcie montaż układu zasilającego projektuje się w miejscu wskazanym na rzutach. Moduły zasilające należy zasilć napięciem ~230V. Zasilanie zostało ujęte w opracowaniu instalacji elektrycznych silnoprądowych.

7.5. Oprogramowanie systemu

Oprogramowanie systemu przywoławczego należy wykonać zgodnie z dokumentacją DTR.

7.6. Pomiary

W trakcie prac uruchomieniowych należy wykonać następujące pomiary:

Pomiary statyczne okablowania: pomiar rezystancji pętli, pomiar rezystancji izolacji (a-b), pomiar doziemienia (a-z i b-z)

7.7. Testy

Po wykonaniu instalacji należy wykonać następujące testy:

- Test poprawności wykonania połączeń.
- Test poprawności wykonania okablowania.
- Test pracy systemu w poszczególnych strefach.

Protokoły z wynikami pomiarów i testów należy załączyć do dokumentacji powykonawczej systemu.

8. Zintegrowany System Bezpieczeństwa

8.1. Ogólne założenia dla systemu

System zarządzania bezpieczeństwem jest systemem otwartym, tzn. umożliwia rozbudowę o nowe elementy systemów bezpieczeństwa i technicznych obiektu. Istnieje przy tym możliwość pracy jednostanowiskowej i sieciowej, z możliwością podziału zadań pomiędzy poszczególne stacje robocze – inne uprawnienia, wizualizacje i komunikaty dla służb ratowniczych, technicznych, ochrony, itp.

System zarządzania bezpieczeństwem umożliwia integrację również innych systemów, które w sposób pośredni lub bezpośredni mogą wpłynąć na szybkość reakcji, wypracowania decyzji i podjęcia stosownych działań przez obsługę zapewniających jej szybką ewakuację z zagrożonego rejonu.

Na potrzeby opracowywanego projektu, w podstawowej wersji, zakłada się integrację systemu PSIM z:

- systemem sygnalizacji włamania i napadu (SSWIN SATEL);
- dźwiękowym systemem ostrzegawczym (DSO PREASIDEO);
- systemem telewizji dozorowej (CCTV NX);
- systemem sygnalizacji pożaru (SSP BOSCH, SSP ESSER);
- systemy gazów medycznych – protokół MODBUS

Ponadto w przyszłości system ma umożliwiać integrację systemów takich jak:

- systemy domofonowe i wideo domofonowe
- abonenckie centrale telefoniczne
- systemy przyzywowe
- systemy szlabanowe
- system automatyki budynkowej BMS
- systemy kontroli dostępu

Oferowany system integrujący PSIM posiada ważną Krajową Deklarację Właściwości Użytkowych, Krajowy certyfikat Stałości Właściwości Użytkowych, Świadectwo Dopuszczenia do stosowania w ochronie przeciwpożarowej wydane przez jednostkę certyfikującą CNBOP, umożliwiające współdziałanie (wizualizację i sterowanie) wszystkich systemów, których działanie lub dezaktywacja jest wymagana w przypadku zagrożenia takich jak:

- centrale wykrywania i sygnalizacji pożaru (centrale SSP);
- dźwiękowe systemy ostrzegawcze (DSO);
- przeciwpożarowe klapy odcinające, klapy odcinające wentylacji pożarowej oraz inne elementy systemów wentylacji pożarowej (np. wentylatory oddymiające);
- systemy wentylacji grawitacyjnej (klapy i okna oddymiające);
- systemy oświetlenia awaryjnego;
- elementy oddzieleń pożarowych (drzwi, kurtyny, bramy);
- urządzenia i systemy stałych urządzeń gaśniczych (zarówno gazowych jak i wodnych);
- inne systemy, instalacje i urządzenia wykorzystywane lub sterowane w czasie stany alarmu pożarowego.

Każde zdarzenie występujące w obiekcie jest protokołowane do pamięci jednostki centralnej systemu. Format zapisu do pamięci uniemożliwia podgląd i edycję danych za pomocą innego programu. Jednocześnie zaistnienie zdarzenia ważnego ze względu na poziom bezpieczeństwa jest protokołowane przy pomocy zewnętrznej drukarki protokołów.

Podczas wystąpienia zdarzenia dzięki podłączonej drukarce raportującej istnieje możliwość wydrukowania mapy architektonicznej z zaznaczonym punktem/czujką na której występuje zdarzenie (lokalizacja) co zdecydowanie skraca czas dojazdu straży zakładowej.

8.2. System Zarządzania Bezpieczeństwem PSIM – zasada działania

System wizualizacji, sterowania i nadzoru, jakim jest system PSIM, zbiera i analizuje sygnały o stanach takich systemów jak: system sygnalizacji pożaru, dźwiękowe systemy ostrzegawcze, system alarmu włamania, system alarmu napadu, system telewizyjnego nadzoru obiektu oraz inne alarmy techniczne.

System Zarządzania umożliwia centralne nadzorowanie wszystkich komponentów automatyki pożarowej, jak i automatyki budynkowej, przedstawienia zdarzeń oraz wspomagania realizacji procedur ich obsługi, w wielu przypadkach całkowicie zastępując operatora w wykonywanych czynnościach.

Będąc systemem otwartym, pozwala dostosować się do rozmaitych urządzeń i systemów, przy czym granice tego dopasowania są bardzo szerokie. Centrala sterująca urządzeniami przeciwpożarowymi, stanowiąca komponent tego systemu, zapewnia nadzór i automatyczną realizację scenariusza na wypadek wystąpienia pożaru. Funkcja ręcznego sterowania zapewnia z kolei na dowolne wystawienie urządzeń w sytuacjach wymagających interwencji człowieka, szczególnie podczas prowadzonej akcji przez JRG PSP. Przydatna jest także podczas prób i testów odbiorowych instalacji bezpieczeństwa.

Podstawę systemu stanowi komputer lub sieć kilku komputerów. Podłączenie central integrowanych systemów do jednego wspólnego systemu informacyjnego zapewnia prostą obsługę, identyczną dla każdego rodzaju centrali. Połączenia takiego można dokonać za pomocą interfejsu dopasowującego standard, według którego komunikuje się centrala z otoczeniem, do standardu, w jakim pracuje system zarządzania bezpieczeństwem.

8.3. Opis funkcjonalny systemu

System PSIM to licencja oprogramowania w której skład wchodzi:

- możliwość dodania do 10 integrowanych systemów (interfejsów)
- 2 000 zawartych w licencji punktów na integrowane systemy. Oznacza to, iż licencja bazowa zawiera w licencji 2 000 elementów liniowych wszystkich integrowanych systemów SSP, CCTV, SSWIN, DSO, które mogą być zdefiniowane w systemie. Elementy liniowe to czujki, moduły pożarowe (każde wejście oraz wyjście traktowane jest jako jeden punkt), ROP (ręczne ostrzegacze pożarowe), punkty pomiarowe i inne urządzenia których stan ma być nadzorowany. Licencje można rozszerzyć do maksymalnie 10 000 elementów liniowych.
- 2 licencje stanowisk operatorskich. Oznacza to, iż system może być obsługiwany jednocześnie na 2 stanowiskach operatorskich.
- 100 procedur. Oznacza to, iż możliwe jest wprowadzenie do systemu 100 procedur działań na wypadek zdarzenia, czyli czynności działania.
- 100 zawartych w licencji planów sytuacyjnych. Oznacza to, iż możliwe jest zdefiniowanie w systemie podkładów budynków, na które nanoszone są czujniki.

Taka wersja systemu gwarantuje przede wszystkim:

- bezterminową licencję, której właścicielem jest obiekt, którego dotyczy wdrożenie;
- analizę napływających alarmów i dowolnych innych informacji z zintegrowanych systemów;
- bezproblemową rozbudowę o kolejny interfejs, budynki, plany sytuacyjne, procedury;
- bezkolizyjną, pogrupowaną, ciągłość napływających informacji;

Zintegrowany System Bezpieczeństwa przede wszystkim wspiera obsługę w przypadku alarmu i gwarantuje realizację następujących funkcji:

- wczesne rozpoznanie zagrożenia za pomocą systemu meldującego,
- szybkie poinformowanie obsługi o nadejściu alarmu,
- podanie propozycji działań do podjęcia z podaniem możliwych środków przeciwdziałania stosownych do danego rodzaju zagrożenia,
- uporządkowanie obróbki zdarzeń z uwzględnieniem priorytetów alarmów,
- odciążenie personelu od czynności rutynowych (praca w tle),
- automatyczne dokumentowanie zdarzeń,
- uproszczenie obsługi często bardzo licznych systemów technicznych i central alarmowych,
- przedstawienie graficznego planu sytuacyjnego – ogólnego oraz szczegółowego – zawierającego lokalizację czujników, dróg dojazdowych, dróg ewakuacyjnych itd.
- automatyczne sterowanie poprzez dany podsystem urządzeniami zabezpieczającymi, takimi jak syreny alarmowe, kamery, urządzenia gaszące itd.
- żądanie potwierdzenia alarmów przez personel, jak również podjęcia czynności oraz dokumentowanie wszystkich działań z sekundową dokładnością (zarówno na papierze, jak i w plikach archiwum, które ponadto mogą być później analizowane)
- cykliczne wykonywanie raportów ze stanu poprawności działania systemów.

Przejrzysty interfejs systemu PSIM, zarządzany w pełni przez przeglądarkę internetową, w sytuacji pojawienia się zagrożenia zapewnia racjonalną, zdecydowaną i bezzakłócenową obróbkę wszystkich napływających informacji. Przy pomocy zintegrowanego interfejsu graficznego z przygotowanymi planami, w przypadku alarmu można szybko np. zlokalizować miejsce jego wystąpienia. Ponadto, odpowiednio skonfigurowany, pozwala by wszystkie dane dotyczące zdarzenia, jak przegrody, drogi ewakuacyjne, odległości, strefy ewakuacji itd. mogły być wizualizowane, przetwarzane i przekazywane.

Nie dopuszcza się instalowania jakichkolwiek aplikacji klienckich na stacjach operatorskich/roboczych. System powinien być w pełni obsługiwany poprzez przeglądarkę internetową. Pozwoli to zapewnić działanie systemu z dowolnego komputera i miejsca, bez konieczności instalacji/pracy serwisanta.

8.4. Struktura systemu (Opracowanie aplikacji graficznej)

System Zarządzania Budynkiem powinien być zbudowany w architekturze klient-serwer (zbudowany na najnowszej platformie technologicznej na poziomie Microsoft.NET) zaimplementowanej w modularnej sieci PC przy użyciu standardowo stosowanych w branży systemów operacyjnych i protokołów sieciowych. System powinien umożliwiać rozproszenie poszczególnych funkcji monitorowania, sterowania, wizualizacji itd. w całej sieci dla uzyskania maksymalnej elastyczności i wydajności.

Proponuje się, aby architektura systemu zarządzania bezpieczeństwem składa się z:

- Dedykowany wirtualny SMS serwer, umożliwiający połączenie i integrację budynkowych systemów technicznych, systemów bezpieczeństwa oraz zapewniający równorzędny dostęp dla stacji operatorskich do wszystkich zdefiniowanych w bazie danych rekordów i zmiennych.
- Urządzenia mobilne (smartphony) powinny posiadać minimalny wymagany system operacyjny Android 5.0 (możliwość obsługi 5 użytkowników)
- Stacja operatorska złożona z komputera stacjonarnego oraz dwóch monitorów 24" dedykowanych dla instalacji technicznych, oparte o komputer klasy PC wraz z oprogramowaniem graficznym będą umożliwiać operatorom dostęp za pomocą przeglądarki internetowej do wszystkich sterowanych i monitorowanych punktów oraz funkcjonować jako podstawowy interfejs systemu zarządzania bezpieczeństwem.
- Przewiduje się dwie stacje operatorskie oraz jedną stację do mobilnego podglądu np. Notebook.
- Switch powinien oferować listy kontroli dostępu ACL, aby chronić wrażliwe elementy sieci przed nieautoryzowanymi użytkownikami.
- W projekcie przewiduje się zarządzane przełączniki sieciowe wyposażono w 16 portów Gigabit Ethernet, które dodatkowo wspierają zasilanie PoE z maksymalnym budżetem mocy 240 W. Powinny wykorzystywać zintegrowane rozwiązania sieciowe, które zmniejszają ryzyko naruszenia bezpieczeństwa, takie jak kontrola dostępu IEEE 802.1X czy zapobieganie atakom typu DoS.
- Do drukowania protokołów musi zostać zainstalowana drukarka.
- Jednocześnie wszystkie zdarzenia muszą być protokołowane na twardych dyskach serwera.
- Proponuje się dostęp operatorów do odpowiednich zasobów systemu oraz możliwość oddziaływania na obsługiwane przez nich urządzenia i instalacje.
- Udostępnianie zasobów serwera dla stacji operatorskiej będzie odbywać się z wykorzystaniem sieci Ethernet LAN/WAN wykorzystującej odpowiednie protokoły komunikacyjne (np. TCP/IP).
- Interfejsy zewnętrzne, zapewniają całościowe zintegrowane sterowanie i monitoring, rejestrację zdarzeń, zdalne powiadomienie alarmowe. Informacje z obiektu są zbierane z wykorzystaniem lub poprzez połączenie urządzeń poprzez wykorzystanie możliwości integracyjnych sterowników, rejestratorów, central sterujących. Komunikacja pomiędzy stacjami operatorskimi a serwerem odbywać się będzie w ramach sieci Ethernet LAN z wykorzystaniem protokołów sieciowych TCP/IP.
- Najważniejszą cechą systemu jest integracja na poziomie jednej wspólnej bazy danych SQL dla całości systemów integrowanych. Zdarzenia, wartości punktów systemowych, alarmy i wszystkie inne parametry dostępne w każdym z systemów: kontroli dostępu, sygnalizacji włamania, systemu sygnalizacji pożaru, muszą znajdować się w jednej wspólnej bazie danych SQL serwera SMS. Stworzenie takiej architektury przechowywania danych pozwala na tworzenie dowolnych interakcji pomiędzy systemami.
- Interfejs użytkownika niezależnie od obsługiwanego systemu musi być identyczny, dostępny bez przełączania pomiędzy programami.
- Z punktu widzenia stacji nadzoru każdy z dostępnych i podłączonych punktów instalacji technicznych w budynku powinien być możliwy do odczytu oraz ewentualnej modyfikacji z poziomu stanowiska operatorskiego przez uprawnionego operatora. System operatorski powinien gwarantować operatorowi maksimum informacji dotyczących obsługiwanych przez niego instalacji.
- Przechodzenie pomiędzy poszczególnymi obrazami i akcje operatorskie powinny odbywać się przy pomocy myszki i / lub klawiatury.
- System projektuje się jako system skalowalny. Oznacza to, że inwestor będzie miał możliwość rozbudowy systemu w sposób dostosowany do rozbudowy obiektu i oczekiwań klienta.
- Do połączenia między systemem bezpieczeństwa a systemami i urządzeniami przeciwpożarowymi system musi wykorzystywać moduł integratora urządzeń przeciwpożarowych. Moduł ten w systemie bezpieczeństwa odpowiada za integrację urządzeń przeciwpożarowych oraz za współpracę tych urządzeń z pozostałymi systemami
- Moduł integratora składa się m.in.. z wyspecjalizowanego komputera przemysłowego , na którym zainstalowane są te elementy programowe systemu bezpieczeństwa, które odpowiadają za komunikację i sterowanie urządzeń i systemów przeciwpożarowych. Moduł integratora zamyka w sobie część przeciwpożarową systemu bezpieczeństwa, co oznacza, że może pracować i realizować swoje zadania bez połączenia z pozostałymi częściami systemu bezpieczeństwa, odpowiadając za obszary nie związane z bezpieczeństwem pożarowym .
- System musi pracować w oparciu o platformę kliencką Microsoft Windows 7, 8 i 10.
- System musi pracować w oparciu o platformy serwerowe Microsoft Windows 2008/2012R.
- System musi mieć możliwość pracy w środowiskach wirtualnych.
- System musi być w pełni obsługiwany, jak i zarządzany, przez przeglądarkę internetową, celem zapewnienia możliwości szybkiej reakcji na awarie sprzętowe – brak instalacji, etc. Oznacza to, iż konfigurowanie, administrowanie, czynności obsługowe systemu oraz bieżąca praca ma odbywać się bez konieczności instalowania dedykowanych aplikacji na stacjach roboczych systemu.
- Nie dopuszcza się instalowania jakichkolwiek aplikacji klienckich na stacjach operatorskich/roboczych. System powinien być w pełni obsługiwany poprzez przeglądarkę internetową.
- System musi zapewniać obsługę flash i JavaScript, jQuery, HTML 5 , CSS3.
- System musi zapewniać możliwość implementacji dowolnych plików htm i html w ramach aplikacji.
- System musi posiadać możliwość pisania skryptów , tworzenia class i metod w celu dowolnego przetwarzania i wizualizowania informacji pozyskanych z integrowanych systemów.
- Sterowniki urządzeń muszą być architektonicznie oddzielone od bazowej aplikacji serwera. Niestabilność SDK systemów trzecich nie ma wpływu na nadrzędną względem nich pracę aplikacji serwerowej systemu bezpieczeństwa.
- Nie dopuszcza się, aby aktualizacja oprogramowania odbywała się w trybie offline. Serwer aplikacji nie może być wyłączony na czas aktualizacji lub modernizacji oprogramowania.
- System bezpieczeństwa powinien posiadać możliwość rozszerzania, poprzez integrację nowych podsystemów. Wymaga się aby obsługa nowych urządzeń realizowana w oparciu o sterownik urządzenia, nie powodowała istotnej aktualizacji systemu prowadzącej do jego przestojów.
- System zarządzania bezpieczeństwem musi posiadać wbudowany moduł projektanta Graficznego Interfejsu Użytkownika (GUI), celem optymalizacji i aktualizacji interfejsów użytkowników, wyświetlanych na stacjach roboczych operatorów (aplikacja kliencka).
- System musi zapewniać swobodne projektowanie układów ramek zawierających elementy dynamiczne i statyczne.
- System musi umożliwiać definiowanie widoku i układu okien, zawierających dowolne treści.
- GUI systemu musi zapewniać możliwość stosowanie dowolnych czcionek, kolorów tła i wypełnień dla podpowiedzi, opisów, etc.
- System musi mieć wbudowany edytor stylów w celu tworzenia własnych motywów.

- System musi umożliwiać przypisanie motywów do operatora bądź stacji roboczej.
- Wszystkie czujniki i elementy wykonawcze poszczególnych systemów (sygnalizowane za pomocą znaku graficznego) powinny zostać rozmieszczone na planach elektronicznych obiektu. W każdej chwili powinna być możliwość określenia stanu wszystkich czujników systemu.
- System poprzez szereg filtrów musi umożliwiać przeszukiwanie czujników względem ich stanu oraz z poziomu tego filtra umożliwić ich grupowe sterownie.
- Serwer systemu zarządzania bezpieczeństwem musi być zasilany poprzez UPS.
- Stacje robocze obsługujące systemy bezpieczeństwa powinny znajdować się w centrum nadzoru obiektu i zasilane powinny być napięciem gwarantowanym.
- System musi pozwalać na generowanie wezwań przez interkom, DSO, telefonię VoIP.

8.5. Urządzenie integrujące wraz z oprogramowaniem – Moduł integratora

System zarządzania budynkiem PSIM składa się z systemu komputerowego, który nadzoruje i steruje elementami wykonawczymi i zintegrowanymi systemami. Taka nadrzędna centrala i zarazem system nadzorująco-sterujący służy do zbierania i protokołowania alarmów i innych informacji z podsystemów. Przygotowuje i przekazuje ponadto wszystkie niezbędne informacje personelowi nadzoru i/lub służbom interwencyjnym. Do połączenia między systemem PSIM, a systemami i urządzeniami przeciwpożarowymi system PSIM wykorzystuje moduł integratora urządzeń przeciwpożarowych. Moduł ten w systemie PSIM odpowiada za integrację urządzeń przeciwpożarowych oraz za współpracę tych urządzeń z systemem PSIM.

Moduł integratora składa się m.in. z wyspecjalizowanego komputera przemysłowego, na którym zainstalowane są te elementy programowe systemu PSIM, które odpowiadają za komunikację i sterowanie urządzeń i systemów przeciwpożarowych.

Moduł integratora zamyka w sobie część przeciwpożarową systemu PSIM, co oznacza, że może pracować i realizować swoje zadania bez połączenia z pozostałymi częściami systemu PSIM, odpowiadającymi za obszary nie związane z bezpieczeństwem pożarowym.

Moduł integratora łączy się z innymi urządzeniami i systemami za pomocą sieci Ethernet lub światłowodowej. Dla systemów i urządzeń wymagających komunikacji poprzez port szeregowy moduł integratora łączy się z innymi urządzeniami przy użyciu modułów NPort. W normalnym stanie budynku (brak wystąpienia zdarzenia niekorzystnego np. pożaru), wszystkie elementy programowe pracują na wspólnym serwerze systemowym zapewniając integrację systemów i instalacji bezpieczeństwa i automatyki budynkowej. Urządzenia przeciwpożarowe komunikują się z modułem integratora, a ten przekazuje informacje do PSIM (physical security information management).

Serwerem odpowiedzialnym za dozоровanie wszystkich systemów jest PSIM, choć stan systemów ppoż. jest także nadzorowany przez moduł integratora. Stacje robocze komunikują się z PSIM. Jeżeli wystąpi zagrożenie bezpieczeństwa wynikające z uszkodzenia infrastruktury komunikacyjnej, stacje robocze (wszystkie lub dedykowane do zadań związanych z ochroną przeciwpożarową) przełączają się automatycznie na komunikację z modułem integratora. Ten ze swojej strony zamiast jedynie pośredniczyć w komunikacji PSIM-systemy ppoż. zaczyna wykonywać działania związane zarządzaniem systemami przeciwpożarowymi. Oznacza to, że serwerem wykonującym działania jest moduł integratora.

Na serwerze oraz w module integratora zainstalowany jest system PSIM. Pozwala to na nieprzerwane monitorowanie wzajemnej aktywności oraz synchronizowanie danych. W przypadku uszkodzenia serwera podstawowego następuje automatyczne przełączenie na moduł integratora.

Po stronie stacji roboczych zdefiniowane zostaną dwa adresy serwerów używanych jako podstawowe i zapasowe. W przypadku uszkodzenia jednego z serwerów, stacja robocza przełącza się automatycznie na drugi serwer i odświeża przeglądarkę. Moduł integratora może działać jako samodzielne urządzenie z pełną funkcjonalnością systemu PSIM dla urządzeń przeciwpożarowych.

8.6. Część graficzna i tekstowa (opracowanie układu graficznego aplikacji)

Plany graficzne, obrysy lub plany sytuacyjne w postaci wektorowej, a więc pozwalającej na prezentację w dowolnej skali, w najlepszy sposób wspomagają służby interwencyjne. Czujniki integrowanych systemów nanoszone są na plany warstwowo, dzięki czemu operator może wygaszać poszczególne warstwy i nadzorować wyłącznie te, które w danej chwili go interesują.

8.7. Nawigacja obiektowa, czyli wprowadzenie układu graficznego i planów akcji

Czujniki przedstawiane są w postaci symboli o różnej, dowolnej wielkości i kształcie. W przypadku wystąpienia zdarzenia czujnik zmienia swój kolor na odpowiedni do rodzaju zdarzenia. Poza wskazaniem stanu za pomocą różnych kolorów i kształtów, dodatkowo można wyświetlić dla każdego czujnika jego najważniejsze dane na planie sytuacyjnym.

Z poziomu planu sytuacyjnego operator może wysterować dane urządzenie. Po kliknięciu w czujnik otwiera się okno panelu obsługi zawierające możliwe przełączenia.

System PSIM posiada wielopoziomowy dostęp do uprawnień połączony z kodami autoryzacyjnymi, dzięki czemu możliwe jest wyświetlanie na danej stacji roboczej tylko wybranych informacji dostosowanych do konkretnego operatora.

Na podstawie koncepcji bezpieczeństwa obiektu, przepisów prawnych i wymagań klienta ustalana jest lista zdarzeń oraz przypisane do nich procedury działań.

Dla usprawnienia pracy ochrony, rutynowe i statutowe zdarzenia alarmowe można zdefiniować w systemie w taki sposób, aby były automatycznie opracowywane i protokołowane bez angażowania osób obsługujących. Lista zdarzeń może być w dowolnym momencie dynamicznie modyfikowana.

W momencie nadejścia informacji o zdarzeniu, system PSIM wspomaga operatora nie tylko szczegółowymi planami sytuacyjnymi z wyszczególnionym alarmującym elementem, ale także wykonuje zdefiniowane procedury automatycznie i prowadzi przez algorytm postępowania dla danej sytuacji. Zadaniem automatycznych procedur działania jest między innymi definiowanie powiązań pomiędzy zintegrowanymi systemami w celu otrzymania kompletnych informacji o miejscu wystąpienia alarmu. Przykładowo, w momencie otrzymania informacji alarmowej, na „monitorze alarmowym” automatycznie prezentowany jest obraz z kamery znajdującej się najbliższej miejsca alarmu lub też w sytuacji alarmu pożarowego system wysyła polecenie sterowania, mające na celu zamknięcie kłap pożarowych.

8.8. Procedury (Wprowadzenie procedur działań i akcji)

Procedury postępowania wprowadzane są do systemu jako algorytmy składające się z pojedynczych działań do wykonania, które można łączyć według arytmetyki Boole'owskiej („i” / „lub”). Algorytmy postępowania zawierają kolejność i opisy czynności, które należy wykonać, ale także m.in. numery telefonów i dane osób, które należy powiadomić o zaistniałym zdarzeniu.

Pojedyncze działanie oznacza krok do wykonania np. „wysłanie ochrony do weryfikacji alarmu”, „powiadomienie szefa ochrony”, „automatyczne otwarcie drzwi”. Operator przez plan działania jest informowany, jakie należy podjąć czynności w przypadku określonego zdarzenia. W tym celu pojedyncze czynności planu są jasno i przejrzysto przedstawiane, muszą być skutecznie wykonane przez operatora, zanim możliwe będzie zdjęcie zdarzenia ze stosów alarmów.

Pojedyncze działania, z którymi zapoznaje się obsługa, mogą być ręczne lub automatyczne. Działania ręczne mogą zawierać dodatkowy opis tekstowy zawierający szczegółowe informacje dotyczące zadania do wykonania a poprzez działania automatyczne może samodzielnie podjąć zdefiniowane akcje mające na celu np. automatyczne połączenie telefoniczne z centrum kryzysowym, wydruk planu sytuacyjnego z alarmującym czujnikiem, dane o zaistniałym zdarzeniu i szczegółowe procedury działania dla służb interwencyjnych, uruchomienie i zamknięcie programów zewnętrznych, protokołowanie czy wysłanie dowolnego dopuszczalnego polecenia sterowania do systemu zewnętrznego itp.

8.9. Zdarzenia alarmowe (konfiguracja filtrów i priorytetów alarmów)

Zdarzenia są wprowadzane na tzw. „stos alarmowy” według przydzielonego im priorytetu z powiadomieniem dźwiękowym i wyświetlane na ekranie aż do momentu zakończenia przez obsługę systemu ich opracowywania.

Opracowanie zdarzenia polega na wykonaniu szeregu działań przez użytkownika. Lista tych działań jest wyświetlana na ekranie i zawiera kolejne kroki obsługi meldunku (zdarzenia) zależne od rodzaju zagrożenia. Kroki te, to np. „sprawdź miejsce zdarzenia w celu zweryfikowania alarmu”. Zestaw kroków może być zaprojektowany przez administratora w bardzo rozbudowanej postaci i możliwe są automatyczne współdziałania integrowanych systemów.

Wybierając zdarzenia do opracowania użytkownik będzie widział plan sytuacyjny tylko z alarmującym czujnikiem, jego opis, czas otrzymania meldunku o alarmie i opisywaną wcześniej procedurę działań, a także działania wykonane automatycznie. Podczas opracowania poszczególnych planów działań operator podawać będzie rezultaty wykonanych działań. Dodatkowo może dodać komentarz. Operator będzie mógł przerwać opracowywanie zdarzenia i ponownie je wznowić. Wszystkie informacje o zdarzeniu i jego opracowaniu (podjętych działaniach) będą protokołowane.

System PSIM przechowuje szczegółowe informacje dotyczące elementu wykonawczego czy sprzętu np. informacje dotyczące montażu, protokoły, instrukcje, daty ostatniej konserwacji i termin następnego przeglądu.

8.10. Moduł analizująco-raportujący

System PSIM może automatycznie zapisywać nie tylko dokładne informacje z przychodzących meldunków, wykonane procedury postępowania i komentarze operatora, ale także pozostałe informacje przesyłane od zintegrowanych systemów czy stacji roboczych. Przechowywane przez system dane historyczne można raportować i analizować wg różnych kryteriów i drukować na formularzach wydruku.

W Systemie Zarządzania Bezpieczeństwem istnieje opcja graficznie przedstawiane raportów w formie wykresów za pomocą modułu analizująco-raportującego. Podając przedział czasowy, możemy uzyskać informację o wszystkich zdarzeniach pochodzących z zintegrowanych systemów.

Moduł raportujący analizująco-raportujący pozwala na analizę zdarzeń pochodzących z integrowanych systemów (awarie, pożary, sabotaże itd.) a także na wizualizację gromadzonych danych w postaci wykresów, zestawień tabelkowych. Po instalacji modułu, w systemie PSIM zostają dodane dodatkowe funkcje związane z graficzną wizualizacją informacji zbieranych przez system PSIM.

Po określeniu przedziału czasu w części wizualizacyjnej pojawi się rozkład meldowanych zdarzeń przez integrowane systemy w postaci wykresu kołowego. Wykres obrazuje ilościowo udział poszczególnych zdarzeń w przedziale czasowym. Po wybraniu konkretnego zdarzenia na ekranie pojawią się dwa wykresy z miesięcznym rozkładem danego zdarzenia w wybranym przedziale czasowym.

8.11. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM BUDYNKU

System zarządzania bezpieczeństwem musi zaoferować możliwości centralnego kontrolowania, rozumianego jako integrację, wizualizację, sterowanie i wyzwalanie interakcji, za pomocą komputera lub kilku komputerów, wszystkimi komponentami techniki zabezpieczeniowej, jak i budynkowej, celem przedstawienia meldunków oraz wspomaganie realizacji procedur ich obsługi, w wielu przypadkach całkowicie zastępując operatora w wykonywanych czynnościach.

Będąc systemem otwartym, pozwoli dostosować się do rozmaitych urządzeń zabezpieczeń, przy czym granice tego dopasowania muszą być szerokie. Podstawą systemu powinien stanowić serwer wraz ze stacją roboczą, względnie sieć kilku komputerów (do zastosowań wielostanowiskowych).

Ponieważ wszystkie nowoczesne centrale sygnalizacyjne wyposażone są w złącze szeregowe lub TCP/IP, należy przewidzieć podłączenie central do jednego wspólnego systemu informacyjnego zapewniającego prostą obsługę. Połączenia takiego można dokonać za pomocą interfejsu dopasowującego standard, według którego komunikuje się centrala z otoczeniem do standardu, w jakim pracuje system zarządzania bezpieczeństwem.

8.12. Wymagania systemu zarządzania bezpieczeństwem

- System musi zapewniać obsługę dowolnej ilości monitorów na stacjach roboczych.
- System musi być rozwiązaniem otwartym, tzn. umożliwiać dalszą rozbudowę o nowe elementy systemów bezpieczeństwa (np. podłączenie nowej centrali włamaniowej itp.).
- Musi istnieć możliwość pracy jednostanowiskowej i sieciowej, z możliwością podziału zadań pomiędzy poszczególne stacje końcowe.

- System zarządzania bezpieczeństwem musi umożliwiać integrację systemów/rozwiązań – systemy podrzędne (minimum): telewizja dozorowa (CCTV), sygnalizacja włamania i napadu (SWiN), sygnalizacja alarmów pożarowych (SSP) oraz nagłośnienia (DSO).
- System zarządzania budynkiem musi posiadać świadectwo dopuszczenia oraz certyfikat stałości właściwości użytkowych, wydane przez CNBOP-PIB, celem zapewnienia możliwości sterowania ewakuacją oraz urządzeniami przeciwpożarowymi, m.in. blokowania i testowania elementów podrzędnego systemu SSP, jak i umożliwienie ręcznego sterowania.
- W systemie zarządzania bezpieczeństwem należy przewidzieć integrację dowolnych czujników (czujniki dwutlenku lub tlenu węgla, czujniki zalania, wilgoci itp.); sygnałów alarmowych (alarmów technicznych) z różnych urządzeń (windy, schody ruchome, bramki parkingowe, sterowniki automatyki klimatyzacji, itp.), stanów parametrów pracy (agregaty prądotwórcze, oświetlenie awaryjne, stacje pogodowe), które zostaną zastosowane w ramach projektu.
- System zarządzania bezpieczeństwem powinien w pełni nadzorować pracę systemu zarządzania budynkiem – analiza parametrów. System zarządzania budynkiem jest podsystemem całościowego Systemu Zarządzania Bezpieczeństwem.
- System musi zapewniać wyświetlenie w czasie rzeczywistym statusu wszystkich systemów z nim zintegrowanych.
- Każde zdarzenie występujące na terenie obiektu musi być protokolowane do pamięci. Format zapisu do pamięci powinien uniemożliwić podgląd danych za pomocą innego programu.
- System musi mieć możliwość definiowania procedur i planów działań, które będą zgodne z przepisami zarządzania bezpieczeństwem w obiekcie. Muszą one wspomagać działanie pracownika Służby Ochrony w podejmowaniu decyzji.
- System musi zapewniać prezentację aktualnego stanu czujników wszystkich systemów bezpieczeństwa, zaś rozmieszczenie czujników na rzutach będących wersją elektroniczną planów budowlanych musi odpowiadać ich rzeczywistej pozycji w obiekcie.
- W systemie wymagana jest możliwość skonfigurowania automatycznego kierowania zdarzeń alarmowych na odpowiednie stanowiska robocze. Dodatkowo wymagana jest możliwość przekazania zdarzenia przez użytkownika. Wymagany jest przy tym mechanizm weryfikacji czy wybrane stanowisko jest aktywne. Przy przekazywaniu zdarzenia wyświetlane są tylko aktywne stanowiska z identyfikatorem (loginem) użytkownika.
- System musi umożliwiać na ponowne przedkładanie zdarzeń po wybranym przedziale czasowym w przypadku zajętości operatora lub w przypadku braku możliwości obsługi zdarzenia.
- W systemie musi istnieć możliwość zmiany obserwowanych planów np. ze względu na poziomy, strefy itp.
- System musi umożliwiać zastosowanie planów wektorowych.
- System zarządzania musi zapewniać pełną dwukierunkową wymianę danych z systemem SSP, KD, DSO oraz SSWiN.
- Wymaga się aby w przypadku zdarzeń alarmowych możliwy był automatyczny bądź ręczny dostęp do nagrań z kamer powiązanych z danym zdarzeniem.
- Wymaga się aby system umożliwiał dowolne tworzenie powiązań między punktami integrowanych systemów, między dokumentami, planami budynku oraz procedurami działań.
- Wymaga się aby z poziomu panelu obsługi punktów integrowanych systemów, był możliwy dostęp do historii punktu oraz dokumentów z nim powiązanych.
- Wymaga się, aby sygnały z systemu kontroli dostępu poprzez zdefiniowane automatycznych procedur działania i automatycznych sterowań, wywoływały działania innych zintegrowanych systemów, np. wykonania zdjęcia, wykonanie nagrania, nadanie komunikatu, wysłanie e-maila, wysłanie sms-a, przesterowanie kamery.
- System zarządzania musi zapewniać dwukierunkową możliwość sterowania systemem CCTV, poprzez pełne sterowanie PTZ, ustawienie kadru, ustawienie zbliżenia, znakowanie obrazu, zapis alarmowy itp. za pomocą klawiszy umieszczonych na planie wyświetlanym na ekranie, jak i za pomocą procedur działań automatycznych np. wskutek naciśnięcia przycisku napadowego, próbę otwarcenia drzwi przez użytkownika nie posiadającego do tego uprawnień w systemie KD, itp.
- Funkcje związane z obsługą kamer muszą być zintegrowane z nadawanym w systemie zarządzania bezpieczeństwem uprawnieniami. System bezpieczeństwa musi zapewniać możliwość ograniczenia poszczególnych działań w oparciu o login i rolę użytkownika.
- Wymaga się, aby system korelował obraz z kamer systemu CCTV, w kontekście dokonanych sterowań i monitorowań (automatyczne przełączenie, wywołanie presetu kamer, kierowanie).
- System zarządzania bezpieczeństwem musi umożliwiać z pulpitu operatora sterowanie zintegrowanymi punktami kamerowymi.
- System musi posiadać własny moduł raportów i wykresów, celem zapewnienia elastycznego raportowania i budowania kokpitów menedżerskich.
- System musi zapewniać możliwość wizualizacji gromadzonych danych w postaci zestawień (tabele) oraz wykresów (linowe, słupkowe, kołowe).
- Raporty i wykresy muszą być integralną częścią systemu, bez konieczności ponoszenia dodatkowych nakładów na zakup, jak i późniejsze utrzymanie.
- System musi umożliwić na tworzenie dowolnych szablonów raportów, związanych z przeszukiwaniem czujników na planach oraz przeszukiwaniem historii ich zdarzeń.
- System musi umożliwić wywołanie szablonu w dowolnym miejscu przez operatora.
- System musi umożliwić export raportów do formatu (CSV, HTML, XML, PDF, Postscript, Excel).
- System musi posiadać graficzny edytor wyboru zdarzeń z bazy danych.
- W ramach systemu PSIM musi być dostęp do dokumentów typu karty katalogowe, protokoły, dokumenty przeglądów serwisowych, dokumenty SLA, instrukcje, etc., wraz z dodatkowymi polami danych (opis, URL) dotyczące każdego urządzenia zwiualizowanego w systemie.

8.13. Możliwości integracyjne

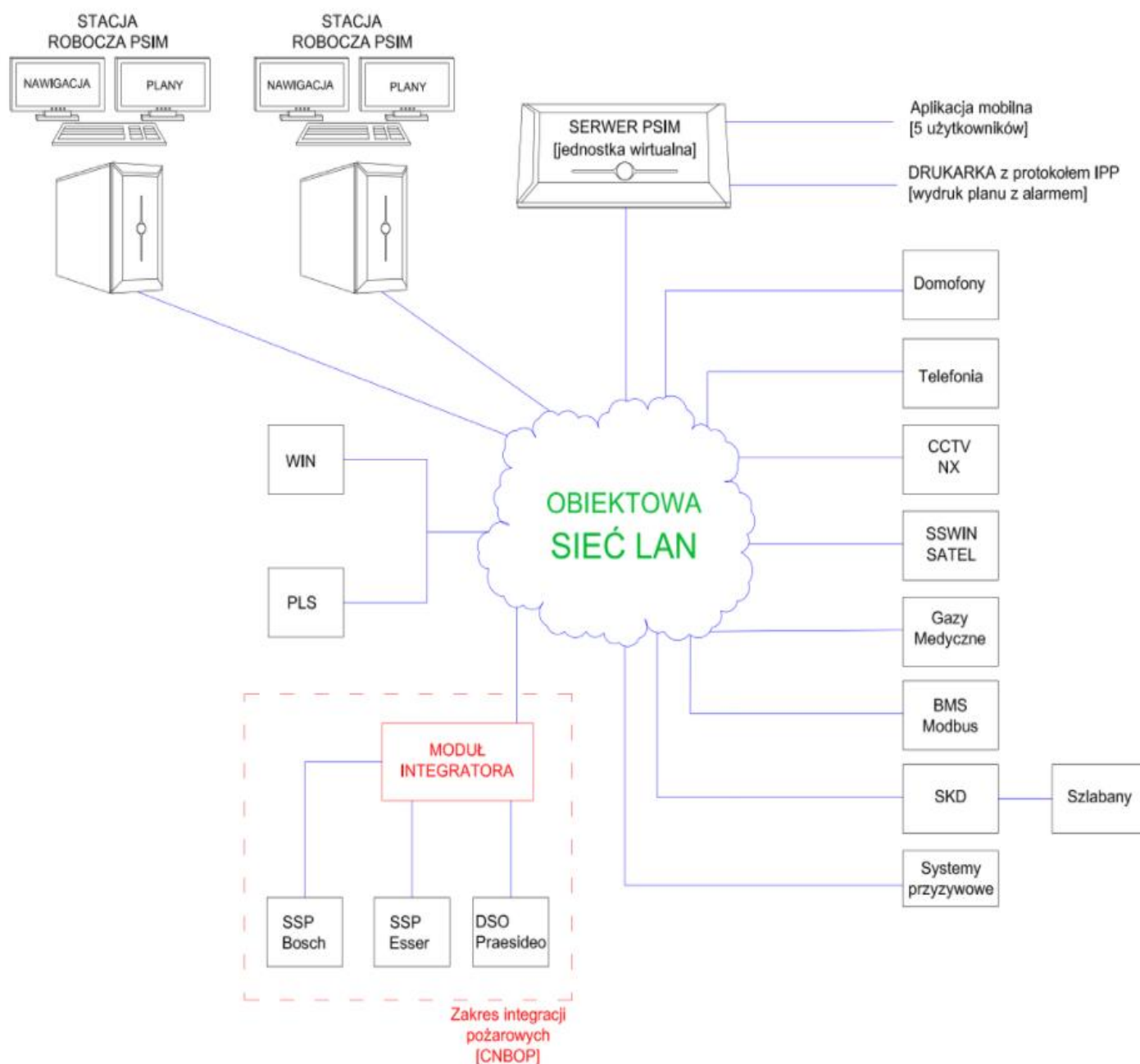
Integracja z systemami odbywa się na poziomie sprzętowym przy wykorzystaniu dedykowanych kart interfejsowych ze specjalnym oprogramowaniem komunikującym się z protokołem urządzenia lub na poziomie programowym, za pomocą protokołów RS-232, RS-485 lub sieci Ethernet.

System Zarządzania Budynkami w każdej chwili można rozszerzyć o dodatkowe funkcjonalności, podłączając kolejne obiekty, centrale, urządzenia czy moduły takie jak: prowadzenie dokumentacji ochronnej, obsługa zdarzeń/incydentów bezpieczeństwa.

W każdej chwili można podłączyć też dodatkowe stacje robocze po to, aby ułatwić operatorom zarządzanie wieloma rozproszonymi obiektami, wyposażonymi w duże ilości czujników i urządzeń.

Dla projektowanego zadania przewiduje się środowisko systemu PSIM działające na wirtualnym serwerze oraz dwie nowe stacje robocze z dwoma monitorami + jedna stacja do mobilnego podglądu.

Poniżej przedstawiono schemat ogólny systemu PSIM



8.14. Integracja z systemem sygnalizacji pożaru

W obiekcie przewiduje się system zarządzania bezpieczeństwem PSIM, który jako system nadzorujący i wizualizujący służy do zbierania i protokołowania napływających alarmów z centrali sygnalizacji pożaru oraz pozostałych informacji pochodzących ze zintegrowanych podsystemów w sposób graficzny z umiejscowieniem na planie architektonicznym. Przygotowuje i przekazuje wszystkie niezbędne informacje personelowi nadzoru. Dzięki czytelnym wizualizacjom umożliwia komfortowe zarządzanie obiektem i upraszcza procedury bezpieczeństwa.

W systemie zarządzania budynkiem musi istnieć możliwość zmiany obserwowanych planów np. ze względu na poziomy, strefy itp. Dla każdego elementu zdefiniowane zostaną procedury działań i określone szczegółowe plany sytuacyjne. Sygnały przesłane przez systemy mogą wywoływać zdefiniowane automatyczne i ręczne procedury działań, które będą znajdować się na planie sytuacyjnym.

W przypadku wystąpienia zdarzenia alarmowego centrala sygnalizacji pożaru inicjuje alarm na niewielkim wyświetlaczu bez możliwości podglądu obiektu w obszarze zagrożonym pożarem. Takie rozwiązanie spawalnia podjęcie odpowiednich działań służb ochrony. W Systemie Zarządzania Budynkiem elementy detekcyjne systemu sygnalizacji pożarowej powinny zostać przedstawione w miejscach zainstalowania na planach sytuacyjnych oraz na planszach zbiorczych.

Taki widok w systemie PSIM wspomaga operatora poprzez wyświetlenie szczegółowego planu sytuacyjnego z naniesioną ikoną elementu, który w danym momencie znajduje się w stanie alarmu, a następnie wykonuje automatycznie zdefiniowane procedury prowadząc jednocześnie operatora przez algorytm postępowania dla danej sytuacji.

Zadaniem automatycznych procedur działania jest między innymi wywołanie dowolnych interakcji między zintegrowanymi systemami np. w momencie powstania alarmu, automatycznie prezentowany jest obraz z kamery znajdującej się najbliższym sąsiedztwie miejsca zdarzenia, wyświetlony zostaje plan sytuacyjny z zaznaczonym aktywnym czujnikiem.

Wartość dodana z integracji:

Operator będzie miał możliwość wykonywania w systemie PSIM czynności zbliżonych do obsługi centrali z poziomu wbudowanego pulpitu, dostępnego na dedykowanej stacji roboczej.

Integracja umożliwi następujące sterowanie systemem SSP:

- wyciszanie wewnętrznego sygnalizatora dźwiękowego
- wyłączanie zewnętrznych sygnalizatorów dźwiękowych
- kasowanie alarmów
- odłączanie pojedynczych czujników lub ROP-ów
- ustawianie pojedynczych czujników lub ROP-ów w tryb testu
- odłączanie grup czujników lub ROP-ów
- ustawianie grup czujników lub ROP-ów tryb w kontroli
- odłączanie wyjścia
- odłączanie wejścia

Integracja umożliwi nadzorowanie następujące elementów systemu SSP:

- stanu topologii i sieci SSP
- stanu poziomu dostępu do centrali
- stanu drukarek
- stanu buzzera
- stanów wejść
- stanów wyjść
- stanów czujników i ROP-ów
- stanu pętli

Od strony sprzętowej do uruchomienia integracji PSIM z SPP ESSER potrzebne są: dwukierunkowy interfejs Essernet SEI wraz z modulem interfejsu RS232 oraz konwerter RS 232 MOXA, na przykład Nport 5110.

W celu integracji z SSP BOSCH centrala musi zostać wyposażona w kartę OPC Server - wymagany firmware centrali w wersji co najmniej 2.0.17. Jedna instancja interfejsu umożliwia integrację z jedną siecią central. Interfejs komunikuje się z siecią central za pośrednictwem karty OPC Server, dostarczonej przez branżę SSP.

Z poziomu systemu PSIM operator może monitorować stany zarówno pojedynczych składowych systemu sygnalizacji pożarowej (na przykład punktowe czujki dymu), jak i całych stref zdefiniowanych w systemie. Interfejs zapewnia komunikację dwustronną – użytkownik informowany jest o alarmach i awariach w systemie, a także może wysyłać rozkazy odłączenia do stref i różnego typu czujek. Możliwe jest również zdalne resetowanie alarmu pożarowego oraz wyłączanie sygnalizacji akustycznej centrali.

8.15. Integracja z Systemem Nadzoru Wizyjnego CCTV

W ramach systemu PSIM proponuje się zwizualizowanie kamer, monitorów, rejestratorów oraz wyjść alarmowych na planach sytuacyjnych oraz na planszach zbiorczych, zgodnie z miejscami ich instalacji.

Centralny serwer BVMS działa jako proxy pomiędzy systemem PSIM, a systemem BVMS. Serwer BVMS musi być obecny, aby wszystkie funkcje interfejsu były dostępne (jeśli obecne są tylko kamery, to interfejs BVMS może oferować tylko niektóre elementy swojej funkcjonalności).

Funkcjonalności do uzyskania w ramach integracji:

- monitorowanie pracy kamer stacjonarnych i obrotowych (np. zgłaszanie awarii) wraz z podglądem na żywo;
- sterowanie kamerami PTZ, na przykład zmiana pozycji, ustawienie presetu (zdefiniowanej pozycji) i zoomowanie;
- monitorowanie pracy rejestratorów NVR i cyfrowych dekoderek;
- sterowanie cyfrowymi dekodernami, na przykład przełączanie sekwencyjne;
- monitorowanie i sterowanie przekaźnikami w kamerach i dekodernach;
- monitorowanie wejść (także wirtualnych) w kamerach i dekodernach;
- tworzenie, definiowanie i edytowanie sekwencji z użyciem np. monitorów, w tym przełączanie monitorów w tryb Quad;
- zapisywanie aktualnego obrazu z kamer poprzez wykonywanie snapshotów;
- rejestrowanie dodatkowych stanów i alarmów z kamer – na przykład wykrywanie ruchu, alarm za ciemnego/jasnego obrazu, zgłaszanie obrazu zaszumionego i zgłaszanie aktywacji nagrywania alarmowego.

Kluczowe zalety z punktu widzenia akcji ratowniczo-gaśniczej:

- Elementy zintegrowanych systemów zgłoszą meldunek z systemów SAP, SSWiN, co spowoduje automatyczne przełączenie kamer.
- Przełączania obrazu z kamer poprzez kliknięcie np. na piktogramy kamer umieszczone na planach sytuacyjnych.
- Automatyczne przełączenie kamery skracza czas reakcji operatora na zaistniałe zdarzenia.
- Śledzenie reakcji osób znajdujących w strefie objętej pożarem.

Wartość dodana z integracji:

- Poprzez integrację z telewizją CCTV w systemie PSIM będzie można tworzyć statystyki związane z analizą obrazu.
- Wykonywanie zdjęć na żądanie bądź w wyniku zdarzenia.
- Dowolne przełączanie kamer i monitorów.
- Wywoływanie „presetów” na kamerach obrotowych.

8.16. Integracja z Systemem Włamania i Napadu

Z poziomu systemu PSIM operator może monitorować stany zarówno pojedynczych składowych systemu sygnalizacji włamania i napadu (na przykład czujki ruchu), jak i całych stref zdefiniowanych w systemie. Interfejs zapewnia komunikację dwustronną – użytkownik informowany jest o alarmach i awariach w systemie, a także może wysyłać rozkazy odłączenia do stref i czujek. Istnieje również opcja przeprowadzania zdalnego resetu alarmów w centrali.

Interfejs do systemu umożliwia wizualizację stanów takich elementów systemu, jak:

- linie,
- grupy,
- czytniki MAX,
- moduły DCM,
- wyjścia,
- klawiatury.

Dodatkowo interfejs umożliwia (za pośrednictwem czujników zbiorczych) wizualizację niektórych stanów dotyczących całego systemu oraz sterowanie systemem alarmowym w zakresie uzbrajania i rozbrajania systemu, oraz uzbrajania i rozbrajania pojedynczych grup.

8.17. Integracja z Dźwiękowym Systemem Ostrzegawczym

Działanie interfejsu polega na okresowym odpytywaniu systemu o stan czujników i, na podstawie odpowiedzi, aktualizowanie ich stanu na serwerze. Możliwe jest również wysyłanie rozkazów do systemu DSO.

Funkcjonalności do uzyskania w ramach integracji:

- monitorowanie linii głośnikowych;
- monitorowanie uruchomienia muzyki tła na strefach;
- monitorowanie załączania komunikatów na strefach;
- włączanie muzyki tła na strefach;
- regulowanie głośności muzyki tła na strefach;
- uruchamianie, kończenie, przerywanie zapowiedzi;
- sterowanie wyjściami;
- kwitowanie awarii na kontrolerze;
- monitorowanie mikrofonów, ekspanderów audio i wzmacniaczy (zgłaszanie meldunków dot. awarii).

8.18. Integracja z systemem gazów medycznych

Działanie interfejsu polega na okresowym odpytywaniu systemu o stan czujników i, na podstawie odpowiedzi, aktualizowanie ich stanu na serwerze.

Funkcjonalności do uzyskania w ramach integracji:

- stan gazów medycznych kanału 1-6 (awaria, alarm max, alarm min, w normie),
- zmierzona wartość ciśnienia/podciśnienia kanału 1-6,
- awaria zasilania głównego

8.19. Moduł Powiadamiania SMS

Moduł współpracuje z systemem PSIM. W ramach zdefiniowanej procedury, wysyła w trybie automatycznym informacje o rodzaju zdarzenia i jego dokładnej lokalizacji. Może funkcjonować również w trybie półautomatycznym, w którym operator dokonuje akceptacji wiadomości SMS wysyłanej na uprzednio zdefiniowany w systemie numer. Może działać w trybie ręcznym, wówczas operator w okienku czynności redaguje treść wiadomości, a następnie wysyła ją do adresata lub adresatów wybieranych z listy rozwijanej. Moduł może być także umieszczony na planie sytuacyjnym jako bramka SMS i obsługiwany przez uprawnione osoby.

Moduł Powiadamiania SMS systemu zarządzania budynkiem PSIM to nowoczesne i funkcjonalne narzędzie, które umożliwia:

- automatyczne wysyłanie powiadomień do uprawnionych osób o wystąpieniu zdarzenia w systemie PSIM
- wysyłanie powiadomień akceptowanych i redagowanych przez operatora do zdefiniowanych osób
- aktualne informacje i bieżącą kontrolę nad sytuacją
- w budynku.

8.20. Moduł MOBILE PSIM

Moduł instalowany na urządzeniach przenośnych wspierających platformę android, rozszerzający funkcjonalność systemu PSIM o zarządzanie zasobami jakimi są patrole mobilne, służby serwisowe, ratunkowe itp.

Kluczowe korzyści:

- szybkie i łatwe przydzielanie zadań na urządzenia mobilne
- efektywne zarządzanie zasobami (patrole, służby techniczne, służby ratunkowe itp.)
- śledzenie pozycji w terenie otwartym oraz wewnątrz budynków
- natychmiastowa informacja o naruszeniu lub przekroczeniu wyznaczonych stref
- raportowanie z możliwością dołączenia dokumentacji multimedialnej

MOBILE PSIM może obsługiwać do 5 użytkowników.

8.21. Integracja z opcjonalnymi systemami bezpieczeństwa

PSIM jest neutralny wobec systemów, które integruje, i funkcjonuje na płaszczyźnie niezależnej od producentów integrowanych przez niego systemów bezpieczeństwa.

Każdy system bezpieczeństwa obiektu, niezależnie od tego, przez jakiego producenta został wyprodukowany, może być zintegrowany z PSIM.

Możliwość włączania obcych technologii staje się zatem ważnym kryterium wyboru systemu.

Poniższa lista pokazuje, jakie systemy różnych producentów można obecnie sprzęgać z systemem PSIM:

- systemy sygnalizacji pożarowej, antywłamaniowe i systemy alarmowania o niebezpieczeństwie,
- nadzorowanie wideo (krosownice wideo ze sterowaniem kamerami, technologia IP),
- systemy kontroli dostępu wraz z systemami RCP, depozytory kluczy,
- systemy komunikacyjne, nagłośnieniowe, DSO, domofony,
- kontrola pracy wartowników,
- windy (wskaźniki stanu i komunikacja z kabiną),
- systemy przywoławcze (analogowe i cyfrowe systemy alarmowania),
- urządzenia elektryczne, rozdzielnie energetyczne,
- systemy głosowej komunikacji radiowej i telefoniczne (te ostatnie z automatyczną identyfikacją i lokalizowaniem rozmówcy),
- systemy synchronizacji czasu,
- sterowanie bramami halowymi, bramami zakładowymi, szlabanami
- sterowanie oświetleniem,
- sterowanie dwustanowe (automatyczne wyłączanie urządzeń i maszyn, włączanie odprowadzania spalin albo odsysania, sterowanie klapami i kanałami).

Na dzień realizacji przedsięwzięcia wymaga się, aby dostawca oprogramowania/producent systemu integrującego posiadał opracowane i w pełni dostępne interfejsy/wtyczki do instalowanych systemów bezpieczeństwa.

9. Uwagi końcowe

- Wszelkie uzasadnione zmiany, które wykonawca chciałby wprowadzić do projektu (na etapie wykonawstwa) muszą być uzgodnione z autorem projektu.
- W pomieszczeniu, w którym zainstalowano centralkę należy umieścić:
- czytelny plan sytuacyjny obszaru dozorowanego,
- opis funkcjonowania i obsługi urządzeń teletechnicznych,
- wskazówki, jak należy postępować podczas alarmów,
- książkę pracy i konserwacji urządzenia.
- Przeszkolenia pracowników obsługujących system teletechnicznych dokona wykonawca po uruchomieniu systemu.
- Po przekazaniu instalacji do eksploatacji, należy zlecić stałą konserwację urządzeń i instalacji – jest to warunek niezbędny do uzyskania gwarancji na eksploatowane urządzenie.
- Użytkownik zobowiązany jest do powiadomienia konserwatora systemu o wszelkich zmianach przeznaczenia pomieszczeń, przebudowach itp. mających decydujące znaczenie w ich zabezpieczeniu.
- Wszelkie prace budowlano-montażowe związane z realizacją niniejszego projektu należy wykonać zgodnie z obowiązującymi normami oraz wytycznymi technicznymi, a w szczególności przestrzegać przepisów BHP,
- Wszystkie 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.
- Wszystkie elementy ujęte w projekcie, a nie ujęte na rysunkach lub ujęte na rysunkach a nie ujęte w projekcie należy traktować tak jakby ujęte były w obu.
- Wykonawca jest obowiązany do wykonania wszystkich prac w załączonym opisie technicznym do projektu. Niezależnie od powyższego Wykonawca jest obowiązany do uzyskania dobrego rezultatu końcowego. Wszelkie niezgodności, ewentualne braki lub niezgodności interpretacyjne dokumentacji w zakresie instalacji teletechnicznych należy uzgadniać z Inwestorem oraz Projektantem.
- Do projektu powykonawczego dołączyć dokumentację DTR oraz niezbędne pomiary.

10. Tabele

Tabela 1	Zestawienie materiałów – Okablowanie strukturalne
Tabela 2	Zestawienie materiałów – Telewizja dozorowa
Tabela 3	Zestawienie materiałów – Kontrola dostępu
Tabela 4	Zestawienie materiałów – System przyzywowy
Tabela 5	Zestawienie materiałów – Instalacja RTV
Tabela 6	Zestawienie materiałów – Trasy kablowe
Tabela 7	Zestawienie materiałów – Zintegrowany system bezpieczeństwa

11. Rysunki

TT-01	Instalacje teletechniczne – rzut piwnicy
TT-02	Instalacje teletechniczne – rzut parteru
TT-03	Instalacje teletechniczne – rzut I piętra
TT-04	Instalacje teletechniczne – rzut II piętra
TT-05	Instalacje teletechniczne – rzut III piętra
TT-06	Instalacje teletechniczne – rzut dachu
TT-07	Instalacje teletechniczne – schemat okablowania strukturalnego
TT-08	Instalacje teletechniczne – schemat telewizji dozorowej
TT-09	Instalacje teletechniczne – schemat kontroli dostępu

TT-10	Instalacje teletechniczne – schemat podłączenia drzwi
TT-11	Instalacje teletechniczne – schemat instalacji RTV
TT-12	Instalacje teletechniczne – schemat instalacji przyzywowej
TT-13	Instalacje teletechniczne – rozlokowanie elementów w pom. techn. +5p