

1	Spis treści	
1	Spis treści.....	1
2	Spis rysunków.....	3
3	Przedmiot inwestycji.....	4
3.1	Inwestor / Zamawiający	4
3.2	Podstawa opracowania.....	4
3.3	Uwarunkowania wstępne stanowiące podstawę opracowania.....	4
3.4	Zakres opracowania.....	5
3.5	Obowiązujące przepisy i normy branżowe.....	6
4	Ogólne założenia projektowanych systemów	7
5	Sieć LAN.....	7
5.1	Kanalizacja teletechniczna dla przyłącza światłowodowego.....	7
5.2	Opis ogólny sieci LAN.....	8
5.3	Normy okablowania strukturalnego.....	8
5.4	Wymagania ogólne dotyczące systemu okablowania strukturalnego.....	9
5.5	Wymagania ogólne dotyczące wykonawcy systemu okablowania strukturalnego.	10
5.6	Okablowanie poziome.....	10
5.7	Punkty dystrybucyjne.....	15
5.8	Zalecenia i szczegółowe wymagania instalacyjne	16
5.9	Pomiary instalacji okablowania strukturalnego	17
5.10	Dokumentacja powykonawcza.....	18
5.11	Wymagania gwarancyjne.....	19
5.12	Specyfikacja przełącznika sieciowego i punktów dostępowych.....	19
6	Instalacja monitoringu wizyjnego CCTV.....	21
6.1	Koncepcja dozoru wizyjnego.....	22
6.2	Struktura instalacji.....	22
6.3	Dobór rozwiązań technicznych.....	23
6.4	Dobór urządzeń.....	23
6.4.1	Kamer stacjonarna zewnętrzna.....	23
6.4.2	Kamera stacjonarna wewnętrzna.....	25
6.4.3	Kamera stacjonarna wewnętrzna do pokoiw miejsca zbrodni.....	25
6.4.4	Kamera zintegrowana z lampą bezcieniową.....	26
6.4.5	Rejestracja wizji	26
6.4.6	Stacja operatora.....	30
6.5	Wytyczne montażowe.....	35
6.6	Zasilanie systemu monitoringu wizyjnego.....	35
7	Instalacja systemu zarządzania bezpieczeństwem - SMS.....	35
7.1	Uwarunkowania wstępne projektowanego systemu.....	35
8	Instalacja systemu kontroli dostępu – SKD.....	42
8.1	Koncepcja sterowania dostępem.....	42
8.2	Dobór zastosowanych rozwiązań – system SKD.....	43
8.2.1	Czytnik zbliżeniowy	43
8.2.2	Kontroler KD	43
8.2.3	Sterownik sieciowy KD	44
8.2.4	Przycisk wyjścia	44
8.2.5	Przycisk ewakuacyjny.....	45
8.2.6	Czujniki kontaktronowe.....	45
8.2.7	Elementy wykonawcze	45
8.2.8	Zasilacze buforowe	45
8.2.9	Oprogramowanie zarządzające systemem KD.....	45

8.2.10 Serwer systemowy	50
8.2.11 Karty bezstykowe autoryzacji dostępu	52
8.2.12 Okablowanie SKD.....	52
8.3 Bilans energetyczny SKD.....	52
8.4 Struktura sieciowa instalacji KD.....	53
9 System parkingowy.....	53
9.1 Koncepcja systemu rozpoznawania tablic rejestracyjnych.....	53
9.1.1 Kamera LPR.....	53
9.1.2 Szlaban elektryczny.....	54
10 Instalacja systemu sygnalizacji włamania SWiN.....	55
10.1 Koncepcja systemu SWiN.....	55
10.2 Wymagania dla projektowanego systemu SWiN.....	56
10.3 Dobór zastosowanych rozwiązań – system SWiN.....	56
10.3.1 Centrala alarmowa.....	56
10.3.2 Szyfrator OLED.....	57
10.3.3 Expander wejść/wyjść z zasilaczem.....	58
10.3.4 Czujniki kontaktronowe.....	58
10.3.5 Detektory ruchu.....	59
10.3.6 Detektory ruchu dualny.....	59
10.3.7 Czujnik zalania.....	59
10.3.8 Zasilanie SWiN.....	59
10.4 Wytyczne montażowe.....	59
11 Wymagania podstawowe integratora pożarowego (SIUP).....	60
11.1 Wymagania podstawowe aplikacji PSIM.....	61
11.2 Cechy funkcjonalno-sprzętowe.....	62
11.3 Prawa dostępu.....	62
11.4 Zarządzania zdarzeniami.....	63
11.5 Operacje kontrolne.....	63
11.6 Grafika.....	64
11.7 Archiwizacja.....	64
12 Instalacja telefoniczna.....	65
13 Okablowanie instalacji niskoprądowych.....	67
14 Wymagania środowiskowe.....	67
14.1 Ogólne założenia.....	67
14.2 Obowiązki wykonawcy.....	69
14.3 Opracowania, do których sporządzenia zobowiązuje się Wykonawcę.....	70
15 Uwagi końcowe.....	73

2 Spis rysunków

- rys. 01T Rzut parteru. Plan instalacji CCTV, okablowania strukturalnego, SSWIN, KD.
- rys. 02T Rzut 1 piętra. Plan instalacji CCTV, okablowania strukturalnego, SSWIN, KD.
- rys. 03T Rzut 2 piętra. Plan instalacji CCTV, okablowania strukturalnego, SSWIN, KD.
- rys. 04T Rzut 3 piętra. Plan instalacji CCTV, okablowania strukturalnego, SSWIN, KD.
- rys. 05T Rzut parteru. Plan instalacji CCTV - kąty widzenia kamer.
- rys. 06T Rzut 1 piętra. Plan instalacji CCTV - kąty widzenia kamer.
- rys. 07T Rzut 2 piętra. Plan instalacji CCTV - kąty widzenia kamer.
- rys. 08T Rzut parteru. Plan instalacji koryt kablowych.
- rys. 09T Rzut 1 piętra. Plan instalacji koryt kablowych.
- rys. 10T Rzut 2 piętra. Plan instalacji koryt kablowych.
- rys. 11T Elewacja szafy dystrybucyjnej.
- rys. 12T Schemat instalacji interkomowej i kontroli dostępu.
- rys. 13T Schemat instalacji SSWiN.
- rys. 14T Schemat blokowy PSIM - integracja systemów.
- rys. 15T Schemat instalacji monitoringu.

3 Przedmiot inwestycji

Przedmiotem opracowania jest projekt techniczny instalacji niskoprądowych dla projektowanego budynku Katedry Medycyny Sądowej Pomorskiego Uniwersytetu Medycznego w Szczecinie na terenie Uniwersyteckiego Szpitala Klinicznego nr 2 przy ul. Powstańców Wielkopolskich 72, 70-111 Szczecin.

3.1 Inwestor / Zamawiający

Pomorski Uniwersytet Medyczny W Szczecinie
ul. Rybacka 1, 70-204 Szczecin

3.2 Podstawa opracowania

- Koncepcja instalacji zabezpieczeń technicznych uzgodniona z Inwestorem,
- Wytyczne Inwestora oraz wielobranżowy projekt budowlany dla niniejszej inwestycji,
- Projekty branżowe architektoniczne i instalacyjne,
- Wieloletnia koncepcja rozwoju systemów bezpieczeństwa PUM,
- Obowiązujące normy i przepisy

3.3 Uwarunkowania wstępne stanowiące podstawę opracowania

Systemy teletechniczne projektowane dla budynku Katedry Medycyny Sądowej Pomorskiego Uniwersytetu Medycznego w Szczecinie wraz z niezbędną infrastrukturą techniczną i zagospodarowaniem terenu przy ul. Powstańców Wielkopolskich 72, w Szczecinie”, stanowią kontynuacją wcześniej zaprojektowanych oraz wykonanych systemów, instalacji i urządzeń funkcjonujących w innych budynkach PUM

Docelowo wszystkie budynki pod względem systemów teletechnicznych będą podlegać integracji i będą stanowiły jeden spójny zintegrowany system. Rozwiązania przyjęte w projekcie dotyczące zastosowanych urządzeń i materiałów podlegały konsultacjom z Użytkownikiem, spełniają powyższe uwarunkowania i zostały przez Użytkownika zaakceptowane do zainstalowania. W realizowanych systemach wymagane jest zapewnienie kompatybilności z systemami Międzywydziałowego Centrum Dydaktyki nr 3 oraz systemami Centrum Symulacji Medycznych. Nie dopuszcza się wprowadzania nie uzgodnionych z Użytkownikiem urządzeń i materiałów innych niż przyjęte w dokumentacji projektowej ze względu na wymóg kontynuacji istniejących systemów.

Wykonawca przed złożeniem oferty zobowiązany jest do szczegółowego zapoznania się z istniejącymi systemami w Centrum Symulacji Medycznych, zastosowanymi tam urządzeniami oraz do konsultacji z Użytkownikiem złożonej oferty, jeśli odbiega ona od rozwiązań przyjętych w dokumentacji projektowej.

Opisane wyżej wymagania dotyczą integracji systemów KD, SWiN, CCTV, systemu zarządzania uczelnią, systemu rezerwacji sal oraz systemu parkingowego, które obecnie są zrealizowane w dwóch budynkach należących do inwestora z wykorzystaniem następujących platform:

- KD – kontrola dostępu iProtect
- SSWiN- system sygnalizacji włamania i napadu – iProtect
- CCTV – monitoring – VDG Sense

- System zarządzania uczelnią – ProAkademia
- System rezerwacji sal – iSRS
- System parkingowy - iProtect

W ramach integracji uzyskano:

- współpracę systemu iProtect z systemem ProAkademia w zakresie importowania danych studentów oraz wykładowców
- odczyt KD z legitymacji studenckiej, albumu wykładowcy oraz karty pracowniczej
- import przez system iSRS planu zajęć z systemu ProAkademia
- aktualizację bazy danych KD i zapis na serwerze iProtect (serwer redundantny)
- integrację systemu parkingowego z systemami KD i CCTV
- objęcie systemem iProtect, VDG, iSRS wszystkich budynków dla wykorzystywania jednej wspólnej bazy danych,
- systemy KD, SSWiN, SAP oraz CCTV posiadają pełną integrację w zakresie pozwalającym na przeglądanie oraz wykorzystanie urządzeń aktywnych między systemami.
- kamery CCTV posiadają integrację z systemem KD dla rejestrowania zdarzeń,
- logowanie użytkownika do jednego adresu sieciowego.

Zgodnie z ustawą o zamówieniach publicznych dopuszcza się zastosowanie równoważnych materiałów i urządzeń w stosunku do przyjętych w dokumentacji projektowej (uwzględniając uwagi powyżej) pod warunkiem zapewnienia parametrów technicznych i funkcjonalnych nie gorszych niż posiadają urządzenia i materiały przyjęte w dokumentacji projektowej oraz zapewniona jest integracja systemów z Centrum Symulacji Medycznych oraz Międzywydziałowego Centrum Dydaktyki nr 3, w zakresie akceptowanym przez projektanta. W takim przypadku wymaga się złożenia stosownych dokumentów uwiarygodniających te materiały i urządzenia oraz ich integrację i kompatybilność z istniejącymi systemami w Centrum Symulacji Medycznych, a ponadto zaakceptowania ich przez Inwestora i nadzór autorski. W przypadku, gdy zastosowanie tych materiałów lub urządzeń wymagać będzie zmiany dokumentacji projektowej, koszty przeprojektowania poniesie wykonawca wprowadzający zmiany.

Uwaga: Po odbiorze instalacji Wykonawca zobowiązany jest przekazać Użytkownikowi protokółarnie, wszystkie hasła i kody dostępu do użytkowanych systemów. Posługiwanie się przez Inwestora hasłami i kodami nie ogranicza i nie pozbawia gwarancji.

3.4 Zakres opracowania

Zakresem niniejszego opracowania jest projekt sieci LAN i instalacji zabezpieczeń technicznych, a w tym:

- KD – kontrola dostępu iProtect
- SSWiN- system sygnalizacji włamania i napadu – iProtect
- CCTV – monitoring – VDG Sense
- System zarządzania uczelnią – ProAkademia
- System rezerwacji sal – iSRS

- System parkingowy - iProtect
- SAP - Polon 6000 wyposażony w SIUP

3.5 Obowiązujące przepisy i normy branżowe

Podczas wykonywania prac budowlanych należy przestrzegać obowiązujących przepisów i norm branżowych, a w szczególności:

- Ustawa z dnia 7 lipca 1994 r. Prawo budowlane (t.j. Dz.U. 2020 poz. 1333);
- Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (t.j. Dz.U. 2019 poz. 1065 z późn. zm.);
- Ustawa z dnia 16 kwietnia 2004 r. o wyrobach budowlanych (t.j. Dz.U. 2020 poz. 215, 471);
- Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (t.j. Dz.U. 2020 poz. 1219, 1378, 1565);
- Rozporządzenie Ministra Środowiska z dnia 14 czerwca 2007 r. w sprawie dopuszczalnych poziomów hałasu w środowisku (t.j. Dz.U. 2014 poz. 112);
- Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (t.j. Dz.U. 2003 Nr 169 poz. 1650);
- Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (t.j. Dz.U. 2020 poz. 961, 1610);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 07 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. 2010 Nr 109 poz. 719);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2009 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych (Dz.U. 2009 Nr 124 poz. 1030);
- Rozporządzenie Ministra Infrastruktury z dnia 18 maja 2004 r. w sprawie określenia metod i podstaw sporządzania kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowanych kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym (Dz.U. 2004 nr 130 poz. 1389);
- Rozporządzenie Ministra Infrastruktury z dnia 2 września 2004 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz.U. 2013 r. poz. 907, 984 i 1047);
- Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz.U. z 2018 r. poz. 1986 z późn. zm.);
- Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. 2020 poz. 256, 695, 1298);
- Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 2019 r., poz. 1231 z późn. zm.);

Normy branżowe:

- PN-EN 60839-11-1:2014-01 Systemy Alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu –

- Wymagania dotyczące systemów i części składowych,
- PN-EN 60839-11-2:2015-08 Systemy Alarmowe i elektroniczne systemy zabezpieczeń – Część 11-2: Elektroniczne systemy kontroli dostępu – Wytyczne stosowania,
 - PN-EN 14846:2010 – Okucia budowlane – zamki i zaczepy elektromechaniczne – wymagania i metody badań
 - PN-EN 50131-1 - Systemy alarmowe – systemy sygnalizacji włamania i napadu – część 1: wymagania systemowe
 - PN-EN 50131-7:2011 - Systemy alarmowe – systemy sygnalizacji włamania i napadu – część 7: wytyczne stosowania
 - PN-EN 50131-6:2019 - Systemy alarmowe – systemy sygnalizacji włamania i napadu – część 6: zasilanie
 - PN-EN 62676-4:2015-06 Systemy dozoru CCTV stosowane w zabezpieczeniach – część 4: wytyczne stosowania

4 Ogólne założenia projektowanych systemów

Podstawowym założeniem projektowanych systemów jest spełnienie wymogów wieloletniej koncepcja rozwoju systemów bezpieczeństwa PUM, a w tym stworzenia zintegrowanego systemu klasy PSIM.

Charakter zrealizowanych budynków Centrum Symulacji Medycznych, budynku Międzywydziałowego Centrum Dydaktyki nr 3 oraz projektowanego Budynku Katedry Medycyny Sądowej, wymusza jakościowe spojrzenie zarówno w obszarze inwestycji CapEx, ale także w kosztach utrzymania obiektu OpEx. Inwestor w swojej Wieloletniej Koncepcji Rozwoju Systemów Bezpieczeństwa w PUM zakłada etapowe przechodzenie na oprogramowanie klasy PSIM oraz zarządzanie obiektem z wykorzystaniem procedur i systemu raportowania.

Docelowo dotyczyć to będzie także innych nie wspomnianych powyżej budynków i obiektów etapowo dołączanych do zintegrowanego systemu klasy PSIM. Efektem zastosowania powyższego systemu będzie uzyskanie efektywnego energetycznie i ekonomicznie budynku, jak również efektywnego i elastycznego funkcjonowania budynku oraz zapewnienie wysokiego poziomu bezpieczeństwa. Dodatkowo system klasy PSIM pozwoli na definiowanie stref i przyporządkowanie użytkowników do tych stref oraz możliwość szczegółowego rozliczania różnych użytkowników budynku, postępowanie wg procedur oraz rozliczanie dzięki transparentnym raportom. Narzędzie klasy PSIM ma pozwalać również na zarządzanie elementami automatyki budynkowej.

Na chwilę obecną Inwestor nie wytyczył jeszcze procedur do zarządzania w obszarze SMS i BMS. Dlatego budowane systemy Kontroli Dostępu, Systemu Sygnalizacji Włamania i Napadu, System Interkomowy, Video Management System oraz urządzeń SAP będą realizowane na serwerze SMS i mają być możliwe do integracji w systemie PSIM. Podobnie w Building Management System, systemy BMS na obecnym etapie będą pracować na dedykowanym rozwiązaniu BMS opisanym w odrębnym opracowaniu.

5 Sieć LAN

5.1 Kanalizacja teletechniczna dla przyłącza światłowodowego

Dla potrzeb przyłącza telekomunikacyjnego projektowanego budynku przewiduje się wykonanie kanalizacji kablowej od istniejącej studzienki pokazanej na planie instalacji elektrycznych przyobiektowych. Kanalizacja

kablowa teletechniczna składać się będzie ze studzienek kablowych SKR2, czterootworowej kanalizacji pierwotnej - rury HDPE 110 oraz kanalizacji wtórnej - rury RHDPE32. Do budowy kanalizacji pierwotnej zastosować rury osłonowe o odporności na ściskanie o wartości 750N, kanalizację wtórną wykonać z zastosowaniem rur o odporności na ściskanie o wartości 250N.

Połączenie projektowanego budynku z istniejącą infrastrukturą teletechniczną wykonać pomocą 2 kabli światłowodowych jednomodowego SM 24J, CPR B2ca.

W zakresie projektu jest wykonanie następujących kabli:

- 2x kabel światłowodowy 24J SM, $l \approx 200(250)m$, relacji projektowana szafa PD1.1 w pom. 1.12 - istniejąca szafa PD w budynku MCD-1,
- 1x kabel miedziany wieloparowy XzTKMXpw 25x4x0.5, $l \approx 200(250)m$ relacji projektowana szafa PD1.1 w pom. 1.12 - istniejąca centrala telefoniczna w budynku MCD-1.

Kable w terenie przyległym do projektowanego budynku układać w kanalizacji która ulega przebudowie - przebudowa ujęta w odrębnej części projektu. Kable na zewnątrz terenu inwestycji układać w istniejącej kanalizacji wykonanej z rur PCV i HDPE.

5.2 Opis ogólny sieci LAN

Głównym punktem sieci LAN dla projektowanego obiektu będą 2 szafy rack zlokalizowana na piętrze w pom. 1.12 serwerownia. Okablowanie poziome do szafy rack wykonać w standardzie kat.6A. Okablowanie poziome zakończyć gniazdami RJ45 kat.6, zastosować po 4 gniazda RJ45 na punkt elektryczno-logiczny.

5.3 Normy okablowania strukturalnego

Podstawą do przygotowania poniższego opracowania są najnowsze wydania norm okablowania strukturalnego. Wszystkie niewymienione w projekcie zagadnienia związane z okablowaniem strukturalnym są regulowane przez poniższe normy:

- ISO/IEC 11801:2017 "Information technology. Generic cabling for customer premises".
- EN 50173-1:2018-07 „Information technology. Generic cabling systems Part 1: General requirements”.
- TIA/EIA 568.2-D:2018 "Balanced Twisted-Pair Telecommunications Cabling and Components”.
- PN-EN 50173-1:2018-07 „Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne”.
- PN-EN 50174-1:2018-08 „Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości”.
- PN-EN 50174-2:2018-08 „Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków”.
- PN-EN 50174-3:2014-02 „Technika informatyczna. Instalacja okablowania. Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków”.

- PN-EN 50346:2004/A2:2010 „Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania”.
- IEC 60512-99-002:2019 „Connectors for electrical and electronic equipment - Tests and measurements - Part 99-002: Endurance test schedules - Test 99b: Test schedule for unmating under electrical load”.
- IEC 14763-4:2021 “Information technology — Implementation and operation of customer premises cabling — Part 4: Measurement of end-to-end (E2E) links, modular plug terminated links (MPTLs) and direct attach cabling”.

5.4 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 przewyższające wymagania kategorii 6A (klasy EA).
- Okablowanie skrętkowe w wersji ekranowanej.
- Certyfikaty wydane przez międzynarodowe, renomowane laboratorium badawcze Force Technology, potwierdzające zgodność okablowania miedzianego z najnowszymi, aktualnymi normami okablowania strukturalnego ISO/IEC 11801:2017, EN 50173-1:2018-07, IEC 14763-4:2021. Należy zapewnić certyfikaty potwierdzające zgodność z normami w zakresie testu całego łącza oraz niezależnych komponentów (kabel, panel, złącze RJ45). Nie dopuszcza się certyfikatów z lokalnych instytutów łączności, ponieważ nie posiadają one wystarczających akredytacji do testów wszystkich parametrów wymienionych w powyższych normach.
- Wszystkie produkty muszą być fabrycznie nowe.
- Celem idealnego dopasowania komponentów, wszystkie produkty okablowania muszą pochodzić z oferty jednego producenta i być oznaczone jego nazwą lub logo.
- Należy użyć szaf 19” tego samego producenta co pozostała część okablowania strukturalnego i oznaczonych jego nazwą lub logo.
- Należy zastosować renomowany i sprawdzony w wielu instalacjach, nie tylko w Polsce, ale i w innych krajach Unii Europejskiej, system okablowania strukturalnego. Należy zastosować przetestowany system, którego producent ma, co najmniej 20-letnie doświadczenie w produkcji okablowania strukturalnego. Zakres jego działalności w całym tym okresie musi obejmować produkcję okablowania miedzianego (kabli skrętkowych, paneli 19”, złączy RJ45), światłowodowego oraz szaf dystrybucyjnych 19”.
- Producent okablowania strukturalnego musi spełniać wymagania międzynarodowej normy odnośnie standardów jakości ISO 9001, należy przedłożyć odpowiedni certyfikat.
- Producent okablowania musi objąć zainstalowany system bezpłatną, 35-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

5.5 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 35 letnią systemową gwarancją niezawodności.

5.6 Okablowanie poziome

Gniazda przyłączeniowe użytkowników (Punkty Logiczne – PL) należy zorganizować w postaci 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).

W gniazdach przyłączeniowych należy zastosować moduły, które powinny umożliwić wpięcie wtyku typu RJ45 (8P8C). Rozwiązanie przecertyfikowane metodą DIRECT PROBING dla kategorii 6A (klasa Ea) przez niezależne laboratorium oficjalnie akredytowane jako: FORCE Technology.

Powinien być również certyfikowany zgodnie z normą IEC 60512-99-002 dotyczącą aplikacji 4PPoE (standard IEEE 802.3bt).

Moduł będzie miał następujące cechy:

- Kompaktowy rozmiar pozwalający na zamontowanie dwóch niezależnych modułów RJ45 keystone, w jednym uchwycie montażowym 45 x 45 mm.
- Należy zastosować komponenty o wydajności kategorii 6A (klasy EA), wg. najnowszych, aktualnych norm okablowania ISO/IEC 11801:2017, EN 50173-1:2018, 6A. Należy zastosować komponenty o wydajności kategorii 6A (klasy EA), wg. najnowszych, aktualnych norm okablowania ISO/IEC 11801:2017, EN 50173-1:2018, TIA/EIA 568.2-D:2018. Moduł powinien zapewniać pracę napięcia wg. najnowszego standardu 4PPoE (przesył mocy do 90W – standard IEEE 802.3bt).
- Należy to potwierdzić certyfikatem z niezależnego laboratorium badawczego (Force Technology).
- Ekranowany moduł z korpusem wykonanym z ZAMAK w dwóch jego częściach, oferujący uziemienie 360°.
- Element modułu służący do terminacji żył kabla zawierający dedykowany wcięcie na drut uziemiający
- Element modułu służący do terminacji żył kabla umożliwiający blokowanie żył poprzez nasunięcie osłony na styk, aby zapewnić najlepsze warunki zaciśnięcia i uniknąć deformacji IDC.
- Zamykanie modułu musi odbywać się poprzez nasunięcie elementu blokującego od boku.
- Kołnierz tylny umożliwiający wprowadzenie kabla instalacyjnego zgodnie z następującymi 5 kierunkami: z prawej, z lewej, od góry, z dołu oraz na wprost. Pozwoli to na dostosowanie złącza do wszystkich rodzajów instalacji (bezpośrednia, natynkowa, podtynkowa itp.) przy jednoczesnym zachowaniu promienia gięcia, a tym samym zapewnieniu optymalnych wartości Return Loss.
- Moduł musi zapewnić instalację kabla o żyłach AWG22 tj. średnica drutu wraz z izolacją < 1,2 mm.
- Odblokowanie złącza w przypadku złego połączenia musi być możliwe, ale też uproszczone i ułatwione.
- Budowa modułu wyposażona w rozdzielacz par, który posiada środkowy separator wzdłużny oraz wypusty separujące ułatwiające rozparowywanie i minimalizujące długość rozkręcania, gwarantujące najlepsze wartości minimalizujące przesłuchy.
- Podwójny obwód PCB do kompensacji sygnałów o wysokiej częstotliwości i zapewniający kompatybilności z komponentem kategorii 6A.
- Moduł wykonany zgodnie ze standardem Keystone,
- Aby uniknąć zwarć, osłona musi być wyposażona w rozwiązanie umożliwiające zaizolowanie przewodów w przypadku zbyt długiego cięcia przewodów.
- Moduł powinien umożliwiać montaż akcesoryjnych, wymiennych zaślepek przeciwkurzowych w przynajmniej 5 kolorach do wyboru w celu zróżnicowania modułów w patchpanelu.
- W celu identyfikacji wybranej partii moduły powinny mieć trwale umieszczony numer seryjny na korpusie.

- Szeroki zakres temperatury pracy od – 40 °C do + 70 °C.
- Żywotność złącza co najmniej 1000 cykli wpięcia wtyku RJ45
- Złącze musi być identyczne na panelach ściennych i na panelach krosowych.

Moduły RJ45 należy montować w 19-calowych panelach rozdzielczych. Panele z zintegrowaną tylną częścią wykorzystane do automatycznego uziemienia na szafach typu RACK 19".

Panel będzie miał następujące cechy:

- System mocowania paneli bez śrub i nakrętek klatkowych: mocowanie dociskowe na szynie 19".
- Wytrzymałość na rozciąganie 110N.
- System blokowania panelu będzie wyposażony w długą metalową prowadnicę umożliwiającą przesuwanie panelu do przodu i z powrotem.
- System wysuwania panelu do przodu powinien umożliwić opuszczenie panelu w dół o przynajmniej 30° w celu łatwiejszego zarządzania modułami.
- Panel będzie wyposażony w otwieralne klapy umieszczone w górnej części w celu umożliwienia montażu złącza poprzez wysunięcie go od góry i od czoła szafy.
- Zainstalowany na górze system kłapek pozwoli każdemu instalatorowi na zmianę modułu od przodu szafy bez konieczności odkręcania elementu montażowych panelu.
- Panel powinien mieć zintegrowany boczny system prowadzenia przewodu z obu stron.
- Klapy przeciwpylowe powinny być wymienne z klapkami oznaczonymi kolorami.
- Dolna klapka etykiety powinna umożliwiać identyfikację portu.
- Panel powinien być wyposażony w obracający się tylny system prowadnic do zarządzania kablami, aby umożliwić ustalenie wybranego kierunku dla wychodzących kabli.
- Tylny system prowadnic do zarządzania kablami powinien być wyposażony w języki ustalające potrzebne do mocowania kabli bez opasek zaciskowych, aby zapewnić dobre wartości strat odbiciowych kabla.

W celu implementacji wydajnych aplikacji, w okablowaniu poziomym przewidziano zastosowanie kabli skrętkowych F/FTP kat. 6A 555 MHz, który przewyższa standardowe wymagania kat.6A i jest przetestowany w paśmie do 555 MHz. Kabel skrętkowy musi zapewniać:

- Niezawodną wymianę danych dla nawet najbardziej wymagających urządzeń końcowych działających z przepływnością 10Gb/s. Należy zastosować kabel o wydajności kategorii 6A (555MHz), który spełnia wszystkie aktualne norm okablowania ISO/IEC 11801:2017, EN 50173-1:2018, TIA/EIA 568.2-D:2018. Należy to udokumentować certyfikatem z niezależnego laboratorium badawczego (Force Technology) potwierdzającym przetestowanie kabla pod kątem spełniania wszystkich wymienionych norm jako komponentu, a nie w układzie całego kanału transmisyjnego. Graniczne wymagania dotyczące wartości parametrów

transmisyjnych:

F(MHz)	TŁUMIENNOŚĆ WTRĄCENIOWA (dB/100 m)	NEXT (dB/100 m)	ACR-N (dB/100 m)	PSNEXT (dB/100 m)	ACR-F (dB/100 m)	PSACR-F (dB/100 m)	TŁUMIENNOŚĆ ODBIĆ (dB/100 m)
1	1,8	90	83	87	87	84	36
4	2,9	88	79	79	86	83	35
10	4,6	86	79	83	83	80	35
16	6,1	85	76	82	82	79	32
25	8,6	84	74	81	77	74	35
31.25	9,1	83	69	80	72	69	34
100	17,3	80	60	77	64	61	33
200	25,5	78	48	75	55	52	32
250	30,5	75	43	72	49	46	31
300	33,6	74	41	71	47	44	28
400	38,0	72	34	69	46	43	24
500	42,5	72	29	69	46	43	22
525	47,0	71	24	68	44	41	20

- Zasilanie urządzeń końcowych (kamer IP, telefonów IP, punktów dostępowych WiFi itd.) wg najnowszego standardu 4PPoE (przesył mocy do 90W – standard IEEE 802.3bt).
- Ekranowanie typu F/FTP w postaci niezależnych ekranów na każdej ze skręconych par, wykonanych z folii aluminiowej oraz dodatkowe ekranowanie w postaci ekranu w postaci folii aluminiowej. W celu podwyższenie skuteczności ekranowania i lepszego uziemienia, co przełoży się na wyższą odporność na zakłócenia, kabel musi być wyposażony w dodatkowy drut drenażowy.
- 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.
- Dodatkowe parametry

Parametr	Wartość
Rezystancja liniowa (maksymalna)	95 Ω / Km
Pojemność wzajemna (maksymalna)	45 pF / m
Nominalna prędkość propagacji (NVP)	79 %
Temperatura pracy	- 20 °C / + 70 °C
Średnica zewnętrzna (maksymalna)	7,4 mm
Średnica żyły miedzianej (minimalna)	0,57 mm (AWG 23)

Zgodnie z dyrektywą 305/2011 - CPR (z ang. Construction Products Regulation), która opiera się na zharmonizowanej normie europejskiej EN 50575:2014 kabel instalacyjny kategorii 6A F/FTP 555MHz musi posiadać klasę CPR – B2ca - s1a d1 a1. Producent okablowania musi posiadać deklarację właściwości użytkowych potwierdzającą klasyfikację kabla.

Dla instalacji systemów bezpieczeństwa budynkowego należy zastosować okablowanie w standardzie kategorii 6A (klasy EA). Kabel instalacyjny systemu bezpieczeństwa budynkowego będzie zgodny ze

standardem kabla sieci LAN. Po stronie punktów kamerowych kable należy zakończyć wtykiem RJ45 posiadającym poniższe parametry i funkcjonalności:

- Zawiera obrotową, łamaną końcówkę RJ45, dzięki czemu idealnie pasuje do portów RJ45, przy których znajduje się mała ilość miejsca.
- Posiada możliwość rotacji -90° (w dół) oraz $+45^{\circ}$ (w górę), celem zminimalizowania promieni gięcia kabla
- Jest w pełni ekranowany.
- Część wtyku RJ45 wpinana do urządzenia oraz część, w której montowany jest kabel instalacyjny musi być połączona elastyczną płytką PCB, zapewniającą wydajną transmisję danych do 10Gb/s.
- Przeznaczony będzie do stosowania nawet na najgrubszych kablach kategorii: 6, 6A, 7. Kontakty IDC muszą pozwalać na montaż żył AWG 26 - AWG 22 (0,40 mm do 0,64 mm) typu drut.
- Zapewnia łatwy montaż bez konieczności stosowania dodatkowej zaciskarki.
- Kolorowe oznaczenia kontaktów IDC celem łatwego rozproawdzenia żył w czasie montażu.
- Posiada parametry kategorii 6A (500 MHz).
- Przenosi zasilanie urządzeń końcowych wg najnowszego standardu 4PPoE wg IEEE 802.3bt o mocy do 90W.
- Umożliwia zbudowanie łącza typu MPTL zgodnie z normą IEC 14763-4:2021.

Kable krosowe RJ45

Zadaniem kabli krosowych RJ45 jest połączenie łączy okablowania poziomego zakończonych na panelu rozdzielczym z portami RJ45 urządzeń aktywnych. W projekcie należy zastosować kable krosowe ze świetlną identyfikacją połączeń, np. typu PatchSee, które zapewnią:

- Transmisję danych dla urządzeń Ethernet działających z przepływnością 10Gb/s. Należy zastosować kabel o wydajności kategorii 6A, ekranowane.
- Idealne dopasowanie do łączy okablowania poziomego, dlatego należy użyć kabli krosowych tego samego systemu okablowania strukturalnego, co pozostałe elementy łączy okablowania. W celu wyeliminowania braku ciągłości w łączach wynikających z niepełnej kompatybilności mechanicznej i elektrycznej nie dopuszcza się użyci kabli krosowych innego producenta.
- Szybką i łatwą lokalizację połączeń w punkcie dystrybucyjnym dzięki świetlnej identyfikacji połączeń. Po podświetleniu jednego końca kabla krosowego zapali się drugi koniec kabla, wskazując połączone porty RJ45 w switchu i na panelu rozdzielczym, przy czym proces ten nie wymaga wypięcia wtyków kabla z portów RJ45. Identyfikacja musi odbywać się za pośrednictwem plastikowych włókien światłowodowych znajdujących się wewnątrz kabla. Nie należy stosować rozwiązań, w których identyfikacja odbywa się za pośrednictwem impulsów elektrycznych przesyłanych wewnątrz kabla i układów elektronicznych (typu diody LED), ponieważ generują one zakłócenia, które powodują błędy w transmisji danych użytkowych, a poza tym w czasie eksploatacji ujawnia się w nich brak ciągłości połączeń w układach podświetlania

LED i wadliwe działanie.

- Kolorystyczne oznaczanie wtyków, w zależności od przeznaczenia kabla. Kolorowe identyfikatory należy nakładać na wtyki RJ45
- Zabezpieczenie wtyku RJ45 przed przypadkowym wypięciem. Kolorowe klipsy nakładane na wtyki RJ45 muszą mieć taki kształt, aby chroniły nosek wtyku RJ45 przed przyciśnięciem i wypięciem. Rozłączenie połączenia musi być możliwe dopiero w momencie wypięcia klipsa ochronnego.
- Elastyczną i wygodną w układaniu konstrukcję wykonaną z 4-parowego kabla skrętkowego typu linka.

5.7 Punkty dystrybucyjne

Do budowy punktów dystrybucyjnych należy użyć szaf 19" tego samego producenta co okablowanie strukturalne i oznaczonych tym samym logo. Główny punkt dystrybucyjny GPD należy wykonać z użyciem szafy serwerowej 47U 800x1000 mm (szer. x gł.). Szafy serwerowe muszą posiadać poniższe cechy i parametry:

- Wytrzymała konstrukcja nawet przy pełnym wypełnieniu urządzeniami, w tym ciężkimi serwerami i UPS-ami. Szafy muszą być przetestowane na nośność co najmniej 1250 kg.
- Szafy nie mogą się chwiać pod obciążeniem, dlatego muszą mieć wzmocnione narożniki, wykonane z jednego kawałka metalu, które łączą elementy ramy szafy. Poszczególne słupy i belki ramy nie mogą być skręcane śrubami bezpośrednio z sobą, gdyż nie zapewnia to ich wystarczającej stabilności względem siebie.
- Zwiększoną nośność należy zapewnić poprzez odpowiednią grubość blachy, co najmniej 2 mm, z której wykonany jest szkielet szafy.
- Drzwi szafy nie mogą się wyginać i falować przy otwieraniu, dlatego muszą być wykonane z blachy co najmniej 2 mm grubości.
- W celu swobodnego dostępu do urządzeń zamontowanych w szafie, nawet w małych pomieszczeniach telekomunikacyjnych i pomiędzy gęsto ustawionymi rzędami szaf, szafa musi posiadać dwuskrzydłowe drzwi z przodu i tyłu, z możliwości otwarcia na 180°. Dzięki temu bez przeszkód będzie można je otworzyć nawet przy ograniczonej ilości miejsca.
- Drzwi przednie i tylne muszą zapewniać swobodny przepływ powietrza chłodzącego serwery, dlatego muszą posiadać perforację w postaci plastra miodu i przewiewnością co najmniej 80%.
- W celu zabezpieczenia urządzeń, drzwi przednie muszą posiadać zamek zamykany na klucz z trzypunktowym ryglowaniem (rygle na górze drzwi, na dole i pośrodku).
- W związku z częstym otwieraniem, drzwi przednie muszą posiadać metalową klamkę, która wytrzyma większą ilość cykli otwarcia w porównaniu z klamką z tworzywa sztucznego.
- Celem przeniesienia szafy nawet przez najwęższe drzwi pomieszczenia telekomunikacyjnego szafa musi posiadać możliwość rozkręcenia szkieletu, a nie tylko zdjęcia osłon.
- Belki 19" muszą posiadać regulację przód tył.
- Celem ułatwienia użytkownikowi oraz instalatorowi identyfikacji miejsca montażu urządzeń, wszystkie belki 19" muszą posiadać trwale

- nadrukowaną numerację jednostek U.
- Szafa musi posiadać w komplecie, zestaw linek uziemiających, dla drzwi i osłon bocznych.
- Szafa malowana proszkowo, kolor antracytowy, RAL 7016

5.8 Zalecenia i szczegółowe wymagania instalacyjne

Instalowanie okablowania strukturalnego

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 stosując łącze typu Permanent Link.
- 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 muszą zostać uziemione.
- W celu ochrony przed niepowołanym 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 S/FTP	10	5	0
Kable U/FTP; F/UTP	50	25	0
Kabel U/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 obowiązują w przypadku prawidłowego uziemienia ekranów kabli transmisyjnych i metalicznych elementów tras kablowych.

Trasy kablowe

Kable należy prowadzić w dedykowanych do tego celu trasach kablowych:

- Okablowanie w pionie między kondygnacjami należy układać w szachtach kablowych i mocować je do drabin kablowych.
- Okablowanie układane w poziomie należy instalować w korytach kablowych lub kanałach kablowych. W głównych trasach kablowych należy stosować podwieszane koryta kablowe metalowe wykonane z blachy perforowanej, które instaluje się w przestrzeni sufitowej.
- Kable skrętkowe i światłowodowe okablowania poziomego instalowane pod tynkiem należy układać w rurach osłonowych z tworzywa sztucznego. Nie należy prowadzić kabli telekomunikacyjnych i zasilających w tej samej rurze osłonowej.
- Połączenia wykonywane na zewnątrz budynków należy realizować przy wykorzystaniu dedykowanej kanalizacji teletechnicznej.

5.9 Pomiary instalacji okablowania strukturalnego

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 łączy typu Permanent Link należy przeprowadzić zgodnie z wartościami granicznymi zdefiniowanymi w ISO 11801 lub EN 50173 oraz dla łączy typu MPTL zgodnie wg normy IEC 14763-4:2021. 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.

Pomiary okablowania miedzianego

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

- Należy przeprowadzić pomiary w układzie pomiarowym typu Permanent Link (bez kabli krosowych).
- Pomiary należy wykonać miernikiem o poziomie dokładności, co najmniej „Level IV”.
- Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łączy, 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 wtrąceniowe - tłumienie (ang. IL - Insertion Loss)
- Straty przesłuchów zbliżnych (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)

Pomiary okablowania światłowodowego

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 wielomodowe (MM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 850 nm i 1300 nm.
- 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 muszą 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.
- do pomiaru okablowania światłowodowego zastosować włókna rozbiegowe o długości 200m.

5.10 Dokumentacja powykonawcza

Po wykonaniu instalacji wykonawca jest zobowiązany do sporządzenia dokumentacji powykonawczej, która będzie zawierała:

- Opis instalacji, przedstawiający architekturę systemu oraz charakterystykę rozwiązań technicznych zastosowanych w systemie okablowania.
- Listę produktów, z ilościami i numerami fabrycznymi o ile takie występują, wykorzystanych do budowy sieci okablowania strukturalnego.

- Schemat oznaczeń łączy miedzianych i światłowodowych.
- Podkłady budowlane z zaznaczeniem: łączy, punktów przyłączeniowych użytkowników oraz punktów dystrybucyjnych.
- Schemat blokowy instalacji.
- Rysunki przedstawiające wyposażenie punktów dystrybucyjnych.
- Pozytywne wyniki pomiarów wszystkich łączy wg normy EN 50173 lub ISO/IEC 11801.
- Certyfikat potwierdzający ważność kalibracji przyrządu, którym wykonano pomiary

Dokumentację należy sporządzić w dwóch kopiach: jedna przeznaczona dla Inwestora, druga przeznaczona dla producenta, celem uzyskania gwarancji systemowej.

5.11 Wymagania gwarancyjne

Inwestor oczekuje, że zainstalowany system okablowania strukturalnego będzie działał niezawodnie przez wiele lat. Dlatego wymagane jest udzielenie przez Producenta 35-letniej systemowej, bezpłatnej gwarancji niezawodności, która zapewni:

- Zgodność ze standardami okablowania strukturalnego obowiązującymi w czasie wykonania instalacji.
- Niezawodne działanie aplikacji (protokołów transmisyjnych), zdefiniowanych w standardach okablowania strukturalnego obowiązujących w czasie wykonania instalacji, dla których system został zaprojektowany.
- Brak wad fabrycznych elementów łączy okablowania oraz błędów w czasie instalacji okablowania.

W tym celu w ciągu 30 dni od daty zakończenia instalacji Wykonawca powinien zgłosić Producentowi potrzebę udzielenia gwarancji i dostarczyć wymaganą dokumentację powykonawczą oraz pomiary sieci okablowania strukturalnego. W ciągu kolejnych 15 dni Wykonawca jest zobowiązany do dostarczenia Inwestorowi certyfikatu gwarancyjnego łącznie ze szczegółowymi warunkami gwarancyjnymi, z uwzględnieniem wymagań zawartych w dokumentacji powyżej.

5.12 Specyfikacja przełącznika sieciowego i punktów dostępowych

Zastosowany przełącznik sieciowy musi posiadać parametry zamieszczone w poniższej tabeli.

Parametr / Minimalna wartość wymagana:	
1.	Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy ze wsparciem dla protokołu 802.3at (PoE+)
2.	Minimum 4 porty 1/10Gigabitowe SFP+ umieszczone z przodu obudowy
3.	Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4.	Wydajność: minimum 130 Mp/s
5.	Bufor pakietów: minimum 7.5 MB
6.	Minimum 8GB pamięci operacyjnej
7.	Minimum 15GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8.	Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9.	Dedykowany port konsoli USB
10.	Port USB 2.0 (niezależny od portu konsoli USB)

11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przysy czym adapter musi pochodzić od tego samego producenta co przełącznik)
12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Dostępne metody łączenia przełączników muszą umożliwiać realizację stosów na odległość co najmniej 300m.
13. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie
14. Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 740W. Pobór mocy (bez PoE) nie może być większy niż 80W.
15. Wielkość tablicy routingu: minimum 2000 wpisów IPv4, 1000 wpisów IPv6
16. Wielkość tablicy ARP co najmniej 8000 wpisów, wielkość tablicy ND co najmniej 8000 wpisów
17. Tablica adresów MAC o wielkości minimum 16000 pozycji
18. Obsługa Jumbo Frames
19. Obsługa sFlow lub Netflow
20. Obsługa skryptów w języku Python
21. Obsługa REST API
22. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.
23. Obsługa RMON (minimum grupy 1,2,3 i 9)
24. Obsługa 4094 tagów IEEE 802.1Q oraz 2000 jednoczesnych sieci VLAN
25. Obsługa standardu 802.1v
26. Obsługa protokołu MVRP
27. Wsparcie dla VXLAN
28. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
29. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
30. Obsługa Secure FTP lub SCP
31. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
32. Obsługa SNTPv4 lub NTP
33. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
34. Obsługa protokołów routingu: routing statyczny, OSPF, OSPFv3
35. Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 1000 grup), MLD (co najmniej 1000 grup)
36. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
37. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
38. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
39. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
40. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
41. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera
42. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
43. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
44. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
45. Wbudowany serwer DHCP
46. Obsługa blokowania nieautoryzowanych serwerów DHCP
47. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
48. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
49. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Co najmniej 5000 wpisów typu ingress i 2000 wpisów typu egress dla IPv4 i MAC
50. Wbudowana sonda IP SLA
51. Zakres pracy od 0 do 45°C
52. Przełącznik w obudowie 19". Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 35 cm.
53. Jeżeli do działania któregośkolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
54. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być

dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.

55. Zaoferowane przełączniki muszą tworzyć spójny ekosystem z posiadanymi przez Zamawiającego urządzeniami Aruba 8325, 6200F, 5406, 5412, a w szczególności posiadać jeden punkt serwisowy.
56. Oferowany przełącznik musi mieć możliwość stackowania z obecnie posiadanymi przełącznikami Aruba 6200F.
57. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.
58. Zamawiający wykorzystuje do monitoringu oraz konfiguracji urządzeń oprogramowanie IMC firmy HP. Urządzenie powinno być na liście wsparcia producenta oprogramowania. Wymaga się licencji pozwalającej na dodanie urządzenia do systemu oprogramowania.

Na rysunkach 01T do 03T pokazano gniazda RJ45 oznaczone symbolem „WiFi”. W miejscach gniazd oznaczonych tymi symbolami zamontować punkty dostępowe o parametrach zgodnych ze standardem Zamawiającego.

6 Instalacja monitoringu wizyjnego CCTV

Przyjęto, iż projektowany system monitoringu wizyjnego będzie wykonany w oparciu o otwarty system zarządzania rejestracją obrazu, oparty o platformę wspierającą różnych dostawców kamer tak aby zaprojektować najlepsze rozwiązanie do utrzymania bezpieczeństwa w obiekcie.

Kompletny system monitoringu wizyjnego będzie składać się z następujących elementów:

- centralnego systemu rejestracji obrazu IP CCTV;
- platformy sprzętowej: rejestratory, serwery i macierze dla IP CCTV;
- infrastruktury sieciowej do transmisji sygnału wideo typu LAN – okablowanie strukturalne i sprzęt aktywny;
- kamer IP;
- systemu zasilania awaryjnego (napięcie gwarantowane);
- stacji operatorskich dla ochrony obiektu dla podglądu dostępnych obrazów;

Platforma monitoringu stanowić będzie dedykowane rozwiązanie spełniające wszystkie wymagane normy będąc niezawodnym elementem, który można integrować z innymi systemami poprzez specjalne oprogramowanie. Równocześnie można je szeroko rozbudować i skalować dostosowując funkcjonalność do wymagań stawianych na obiekcie. Platforma ma możliwość zaimplementowania kamer różnych producentów poprzez wbudowane pełne sterowniki kamer (pełna kontrola wejść/wyjść alarmowych, audio, sterowanie PTZ, itd.). Oprogramowanie będzie obsługiwać protokoły ONVIF w wersji co najmniej 2.0 oraz protokół PSIA.

Platforma musi zapewnić obsługę min. 40 producentów kamer i koderów na bazie autorskich dedykowanych protokołów tych producentów, aby zapewnić jak największą elastyczność oraz możliwość doboru jak najlepszego urządzenia spełniającego wymagania ekspozycji, transmisji itp. w danym punkcie kamerowym.

W przypadku braku wspierania dedykowanego protokołu dopuszcza się możliwość stosowania protokołów generycznych takich jak ONVIF oraz PSIA w

celu połączenia urządzenia z platformą. System musi wspierać obsługę protokołu ONVIF G, S, T. Producent systemu VMS musi być członkiem stowarzyszenia ONVIF przynajmniej na poziomie: Full Member.

Wymagane jest obsługiwane wbudowanych w kamerę algorytmów badania i jakości obrazu kamery w celu ułatwienia zarządzania wielokamerowymi systemami poprzez automatyczne poinformowanie operatora i administratora o utracie jakości obrazu.

Serwer systemu CCTV musi zapewniać możliwość obsługi do 500 urządzeń w tym kamer, kanałów video i koderów video oraz obsługę połączenia kodaera, dekodera, klawiatury CCTV i moduły we / wy.

Producent systemu musi zapewnić zgodność z europejskimi aktami prawnymi min. RODO, NIS2 a także zapewniać wsparcia w działaniach w systemie w tej samej strefie czasowej.

6.1 Koncepcja dozoru wizyjnego

Przyjęto następujące założenia, stanowiące podstawę opracowania:

- instalacja dozoru wizyjnego ma na celu monitorowanie:
 - wejść do budynku
 - wejścia o ograniczonym dostępie
 - wewnętrznych dróg komunikacyjnych,
 - istotnych pomieszczeń i obszarów (serwerownia),
- system oparty o urządzenia (kamery, rejestratory) IP, zasilanie kamer z przełączników PoE,
- ochrona kamer zewnętrznych ochronnikami przeciwprzepięciowymi,
- jako okablowanie sygnałowe zastosowane będą kable skrętkowe i światłowodowe (projekt instalacji teletechnicznych).
- szafy dystrybucyjne oraz urządzenia w nich zlokalizowane będą zasilane z wydzielonych obwodów 230VAC [napięcie gwarantowane podtrzymywane zasilaczami UPS i agregatem prądotwórczym – projekt instalacji elektrycznych].

Rozmieszczenie kamer pokazano na podkładach budowlanych.

6.2 Struktura instalacji

Zgodnie z przyjętymi założeniami wstępnie zakłada się instalację następujących urządzeń:

- Kamery o min. rozdzielczości 5mpix w obudowach kopułkowych wyposażone w oświetlacze IR dozoru wewnątrz korytarze poczekalnie oraz dozoru przejścia wewnątrz w budynku
- Kamery o min. rozdzielczości 5mpix w obudowach kopułkowych wyposażone w oświetlacze IR dozoru min. pom. Sali sekcijnej ; Sekcji Biologicznej;
- Kamery o min. rozdzielczości 5mpix w obudowach bullet wyposażone w oświetlacze IR na zewnątrz budynku
- Przewiduje się 2 niezależne serwery rejestrujące:
 - jeden serwer dla kamer dozoru oznaczonych jako K3 oraz KZ ,
 - drugi serwer dla kamer w strefach sekcyjnych oznaczonych jako K1 i K2 oraz kamer K4 w pokojach miejsca zbrodni,
- Rejestracja wizji odbywać się będzie na serwerach sieciowych, o wydajnościach dobranych odpowiednio dla oczekiwanego strumienia

wizji z zaprojektowanych kamer oraz oczekiwanego czasu rejestracji dla zaproponowanego profilu rejestracji (jakość kompresji, ilości nagrywanych klatek/ sek, harmonogramy, detekcja ruchu, itp.) Na serwerach musi istnieć możliwość wydzielenia odpowiednich strumieni z kamer

- Monitorowanie w pomieszczeniu ochrony odbywać się będzie za pomocą dedykowanych wielomonitorowych stacji klienckich,
- Podgląd z kamer w strefach sekcyjnych i pokojach miejsca zbrodni będzie odbywał się na dedykowanej osobnej stacji operatorskiej
- Instalowanie urządzeń IP wymusza włączenie ich w budynkową (w dedykowanej części) sieć ethernet. Sieć taka powinna spełniać wymogi odpowiedniej przepustowości, a urządzenia aktywne (switche) powinny zapewniać zasilanie kamer za pomocą standardu PoE:
 - [802.2at] dla kamer wyposażonych w oświetlacze IR oraz grzałki,
 - [802.2af] dla kamer wewnętrznych,

Zasilanie awaryjne – zapewnione będzie zasilanie awaryjne systemu CCTV z sieci z podtrzymaniem napięcia i rezerwowym zasilaniem minimum do czasu uruchomienia z agregatu prądotwórczego. Zasilacze UPS dla urządzeń i w lokalnych węzłach będą zapewniać ok.15 minut podtrzymania zasilania instalacji elektrycznych].

6.3 Dobór rozwiązań technicznych

Wizja z projektowanych kamer będzie rejestrowana w centralnym systemie rejestracji obrazu IP CCTV na serwerach przewidzianych dla kompletnego systemu. Zainstalowany serwer umożliwi integrację instalacji projektowanego budynku z instalacjami innych budynków wybudowanych i będących w realizacji.

Serwer dla kamer dozoru zostanie zlokalizowany w serwerowni pom. 1.12 na 1 piętrze. Serwer dla kamer sekcyjnych i pokoi miejsca zbrodni zostanie zlokalizowany w tym samym pomieszczeniu serwerowni. Dla monitorowania wewnętrznych i zewnętrznych stref w budynku zastosowano kamery o rozdzielczości 5Mpx założono wykorzystanie kodeka H.265.

Kamery zainstalowane w budynku medycyny sądowej PUM wykorzystywane będą głównie podczas codziennej pracy, przyjęto ciągły czas rejestracji, szybkość rejestracji 6kl/s. przy załączonej detekcji. Dla kamer w pomieszczeniach specjalnych typu sala sekcyjna, sekcja biologiczna założono szybkość rejestracji 25kl/s. podczas detekcji ruchu.

Dla budynku Medycyny sądowej PUM przyjmuje się 30 dni dla przechowywania materiałów archiwalnych. Należy zapewnić ustawienia serwera w trybie RAID 6.

6.4 Dobór urządzeń

6.4.1 Kamer stacjonarna zewnętrzna

Kamera stacjonarna tubowa [obudowa zintegrowana bulet]

- Rozdzielczość min: 5 Mpx
- Kompresja MJPEG, H.264 oraz H.265
- Prędkość odświeżania 30 kl/s
- Minimalne kąty widzenia przy 5 Mpx: 31,5° do 102,1° w poziomie, 22,7°

- do 70,3° w pionie
- Obiektyw P-IRIS sterowany zdalnie, ogniskowa 2,7-12mm, mechaniczny filtr IR
- Dynamika 120db
- IK10 oraz IP66”.
- Wbudowany żyroskop, EIS
- Zasilanie 24Vac, 12Vdc, PoE IEEE 802.3at (max.13,6W)
- Temperatura pracy -55 C..+60 C
- Zgodność z sekcją 889 NDAA

Kamera dla rozpoznawania tablic rejestracyjnych

Parametry techniczne	
Temperatura użytkowania i przechowywania	-40°C do + 60°C
Wilgotność użytkowania i przechowywania	Do 95%, bez kondensacji
Pobór energii	25W
Waga	1,5kg
Wymiary	178 x 90 x 133 mm
Napięcie zasilania / zasilacza	24 Vdc, PoE+
Kamera	
Kamera ANPR (ALPR)	2MP w skali szarości
WiFi	Opcjonalnie
Przechowywanie	SD do 128GB
Złącze wandaloodporne	TAK
IK	IK09
Podświetlacz IR	8 diod LED na podczerwień o dużej mocy
Obiektyw	Stały obiektyw do wyboru
System operacyjny	LINUX
Wejścia / wyjścia cyfrowe	2 wejścia optoizolowane - 2 wyjścia przekaźnikowe - 1 wyjście stroboskopowe
Ethernet	GigaBit Ethernet 10/100/1000
IP	IP67
Zarządzanie	
Integracja	Instalacja i konfiguracja z wbudowaną aplikacją internetową
Serwer Web	Instalacja i konfiguracja z wbudowaną aplikacją internetową
Data i godzina	Synchronizacja za pomocą protokołu NTP
Aktualizacja oprogramowania	Aktualizacja za pośrednictwem aplikacji sieci Web i protokołów integracji
Parametry analityczne	
OCR	Silnik ANPR (ALPR)
Ilość obsługiwanych linii	1
Platforma programowania	Stark

Akcelerator AI	1 akcelerator sprzętowy
Maksymalna prędkość pojazdu (km/h)	Do 70 km/h
Odległość robocza (m)	Do 25
Wykrycie	99,5%
Odczyt	> 95%
AES256	Tak
SHA2	Tak
Kompresja	JPG
Dane dotyczące działania	
Tryby wyjść	HTTP, HTTPS, FTP, SFTP, TCP RAW, komunikacja szeregową, pamięć lokalna
Formaty wiadomości	W pełni konfigurowalne formaty wiadomości, w tym JSON, XML, niestandardowy ciąg
Konfiguracja	Konfigurowalne zdarzenia/akcje i metadane
Port szeregowy	Tak, półdupleks RS485
Wyjście cyfrowe	Tak
Serwer FTP	Tak, dostęp do partycji pamięci masowej
Tryb wyzwalania	Przechwytywanie i przetwarzanie obrazu wyzwalane przez Ethernet i sygnał cyfrowy
Automatyczne wyzwalanie	Samoczynne wyzwalanie w oparciu o analizę obrazu AI, wykrywanie aut bez tablic
Wiegand	Tak

6.4.2 Kamera stacjonarna wewnętrzna

Kamera kopułowa wandaloodporna

- Rozdzielczość min: 5 Mpx
- Kompresja MJPEG, H.264 oraz H.265
- Prędkość odświeżania 30 kl/s
- Minimalne kąty widzenia przy 5 Mpx: 31,5° do 102,1° w poziomie, 22,7° do 70,3° w pionie
- Obiektyw P-IRIS sterowany zdalnie, ogniskowa 2,7-12mm, mechaniczny filtr IR
- Dynamika 120db
- IK10 oraz IP66”.
- Wbudowany żyroskop, EIS
- Zasilanie 24Vac, 12Vdc, PoE IEEE 802.3at (max.13,6W)
- Temperatura pracy -55 C..+60 C
- Zgodność z sekcją 889 NDAA

6.4.3 Kamera stacjonarna wewnętrzna do pokoiw miejsca zbrodni

W pokojach miejsca zbrodni 2.16 i 2.17 zlokalizowanych na 2 piętrze zamontować po 2 kamery HD 8Mpx z wbudowanym oświetlaczem IR, zapewniającym ostry obraz w rozdzielczości 4K nawet w trudnym oświetleniu.

- Rozdzielczość 4K, min: 8 Mpx
- Kompresja MJPEG, H.264 oraz H.265
- Prędkość odświeżania 30 kl/s

- Minimalne kąty widzenia: 113° (Szeroki) do 59° (Tele)
- Obiektyw zmienny elektrycznie obiektyw zmiennoogniskowy 4 do 8 mm, f/1.6
- Dynamika 120db
- IK10 oraz IP66.
- Zasilanie 24Vac, 12Vdc, PoE IEEE 802.3at (max.13,6W)
- Temperatura pracy -55 C..+60 C
- Zgodność z sekcją 889 NDAA
- Możliwość rejestracji dźwięku

6.4.4 Kamera zintegrowana z lampą bezcieniową

Kamera montowana w lampie bezcieniowej będzie integralną częścią lampy i będzie dostarczona przez dostawcę lamp bezcieniowych. Parametry kamery będą opisane wraz ze specyfikacją lampy w projekcie technologii.

Podstawowe parametry kamery:

- Rozdzielczość 4096x2160
- Standard Wideo 4K ultra HD
- Możliwość rejestracji dźwięku
- Wyjście wideo HDMI 1.4, 6G SDI

Kamery w lampach bezcieniowych mają wyjście HDMI, w związku z tym konieczne jest zastosowanie dla kamer enkoderów o parametrach:

- Wejścia: 1x HDMI (żeński typ A), 1x wejście audio analogowe
- Wyjścia: 1x RJ-45 Cat5e/6 (100M/1000M), 1x HDMI loop out
- Wspiera kodowanie H.264 oraz H.265
- Wspiera protokoły UDP, HTTP, RTP, RTSP, RTMP(S), SRT, unicast i multicast.
- Bitrate wideo: 16Kb/s ~ 12Mb/s
- Bitrate audio: 24Kb/s ~ 320Kb/s
- Gigabitowy interfejs sieciowy
- Wspiera rozdzielczości wejściowe do 1080p 60Hz
- Wspiera zmianę parametrów przesyłanego obrazu (skalowanie, zmiana odświeżania: 5 – 60 kl./s)
- Obsługuje sygnał z HDCP 1.4
- Wsparcie ONVIF
- Interfejs WEB do zarządzania
- Przesyła jeden główny stream i jeden sub-stream

6.4.5 Rejestracja wizji

Serwer strumieni wideo, spełniający następujące warunki:

- Czas przechowywania zarejestrowanego materiału powinien zależeć jedynie od przestrzeni dyskowej
- Zgodność z ONVIF i PSIA
- Możliwość obsługi za pomocą platform mobilnych takich jak Android, iOS, Windows Mobile oraz poprzez przeglądarkę internetową,
- Możliwość zapisów sygnałów wizyjnych na wewnętrznych dyskach serwerów zapisu oraz macierzach DAS (Direct Attached Storage), NAS (Network Attached Storage) i SAN (Storage Area Network)
- Funkcja zarządzania alarmami generowanymi przez system w tym:

- Zdarzenia systemowe takie jak, błędy rejestracji oraz archiwizacji
- Zgodność z sekcją 889 NDAA

Aplikacja do przeglądania materiału wizyjnego powinna umożliwiać:

- Podgląd kamer z różnych rejestratorów
- Definiowanie publicznych i prywatnych widoków
- Widok pełnoekranowy
- Wyszukiwanie nagrań po czasie i dacie
- Zmiana szybkości odtwarzania zarejestrowanego materiału
- Cyfrowe zbliżenie w widoku na żywo oraz podczas odtwarzania
- Definiowanie dostępu do aplikacji w zależności od pory dnia.
- Wyszukiwanie kamer i widoków
- Predefiniowane widoki w proporcjach obrazu 4:3 oraz 16:9
- Widoki przystosowane do kamer obserwujących pionowe i szerokie obszary
- Funkcja podwójnego uwierzytelniania
- Obsługa multicast
- Obsługa sekwencji
- Możliwość tworzenia przycisków na widokach
- Możliwość odświeżenia widoku z kamery na podstawie detekcji ruchu
- Niezależne odtwarzanie wielu kamer w ramach jednego widoku
- Wybór widoków za pomocą predefiniowanego skrótu klawiszowego
- Wyszukiwanie nagrań w oparciu o detekcję ruchu oraz zakładki
- Zarządzanie alarmami
- Eksport nagrań do formatu natywnego z możliwością dołączenia odtwarzacza
- Eksport nagrań do formatu AVI
- Eksport nagrań zabezpieczony hasłem
- Możliwość blokady eksportu z wyeksportowanego już materiału
- Informacja o szacowanym rozmiarze eksportowanych nagrań
- Możliwość tworzenia masek prywatności na eksportowanych nagraniach

System powinien zapewniać:

- Obsługę wyszukiwania nagrań na podstawie detekcji ruchu na zarejestrowanym materiale
- Obsługę następujących formatów: MJPEG, MPEG-4 SP, MPEG-4 ASP, MxPEG, H.264 oraz H.265
- Obsługę strumieni w trybie Variable i Constant Bit Rate
- Zapis w trybie ciągłym i zdarzeniowym, z uwzględnieniem harmonogramów
- Aktualizacja obsługiwanych kamer powinna się odbywać poprzez aktualizację bazy danych sterowników i nie może skutkować reinstalacją systemu.
- Obsługa połączeń HTTPS oraz SSL
- Zapis obrazów z kamer z gęstością uzależnioną jedynie od możliwości samej kamery
- Wbudowany, niezależny od kamery, system detekcji ruchu w czasie rzeczywistym

- Możliwość pobierania wielu różnych strumieni z jednej kamery.
- Obsługa detekcji ruchu w całym kadrze kamery lub tylko w zdefiniowanej części
- Możliwość zdefiniowania odstępu pomiędzy pełnymi klatkami w kodekach MPEG4/H.264
- Możliwość nagrywania jedynie klatek kluczowych używając kodeków MPEG4/H.264
- Możliwość tworzenia profili czasowych oraz reguł zdarzeń, na podstawie których będą mogły być wykonywane akcje systemowe.
- Obsługa profili powiadomień pozwalających na wysyłanie informacji o zdarzeniach systemowych. Powiadomienia email powinny mieć możliwość dołączenia obrazów w formacie JPEG, nagrań AVI.
- Możliwość dystrybucji strumienia z kamery pomiędzy komputerami z zainstalowaną aplikacją kliencką
- Software Development Kit (SDK), który zapewni możliwość integracji systemu z aplikacjami innych dostawców
- System powinien działać jako agent SNMP pozwalający na generowanie trapów SNMP
- Możliwość tworzenia kont użytkowników bezpośrednio w systemie.
- System powinien umożliwiać tworzenie zakładki w trybie odtwarzania oraz na żywo, Funkcja zakładki powinna umożliwiać:
 - Ręczne tworzenie zakładki przez operatorów
 - Możliwość edycji, wyszukiwania oraz usuwania zakładki
 - Stworzone zakładki są zaznaczone na osi czasu w trybie odtwarzania
- System powinien obsługiwać funkcję mapy, która przedstawia w intuicyjny sposób miejsce rozmieszczenia poszczególnych urządzeń systemu (jako podkłady map grafiki w następujących formatach: JPG, GIF, PNG i TIF)
- Mapy powinny mieć możliwość definiowania aktywnych obszarów, tzn. połączeń pomiędzy innymi mapami
- Funkcja mapy powinna umożliwiać podgląd kamery po najechaniu myszą na ikonę kamery na mapie
- Funkcja mapy powinna umożliwiać rysowanie obszarów na mapie obrazujących orientacyjny kadr kamery stałopozycyjnej
- System powinien zapewniać funkcję zarządzania alarmami. Funkcja alarmu powinna umożliwiać:
 - Tworzenie czasowych profili alarmowych
 - Generowanie alarmów na podstawie zdarzeń systemowych
 - Możliwość dodawania instrukcji postępowania oraz przydzielania właściciela alarmu
 - Możliwość definiowania priorytetów, kategorii, statusów, ostrzeżeń dźwiękowych oraz kodów zamknięcia alarmu
 - Integracja alarmów z funkcją mapy. Alarmy dotyczące urządzeń naniesionych na mapę powinny odzwierciedlać stan urządzenia na mapie.
 - Możliwość eskalowania i przypisywania alarmów do innych użytkowników
 - Możliwość automatycznego odtwarzania z poziomu edycji alarmu zarówno podglądu na żywo jak i również materiału zarejestrowanego

- z momentu rozpoczęcia alarmu
- System powinien umożliwiać tworzenie stref prywatności
- System powinien umożliwiać wielostopniową archiwizację zarejestrowanego materiału,
 - Przechowywanie nagrań w wielu zasobach sieciowych
 - Przenoszenie nagrań pomiędzy zasobami sieciowymi w oparciu o harmonogram
 - Możliwość zdefiniowania czasu przechowywania nagrań dla każdego z zasobów sieciowych
 - Możliwość konfiguracji czasu przechowywania nagrań po upływie, którego to będą one kasowane
 - System umożliwia przypisanie urządzenia do odpowiedniego zasobu sieciowego na którym będą rejestrowane dane
- System powinien umożliwiać szyfrowanie materiałów eksportowanych
- System powinien umożliwiać podwójną autoryzację użytkowników
- Możliwość podglądu i tworzenia raportów o wydajności serwera zarządzającego oraz rejestratorów, co najmniej dotyczące użycia procesora, pamięci RAM, zajętości przestrzeni dyskowej, użycia sieci
- Możliwość generowania raportów o konfiguracji systemu
- System powinien udostępniać funkcję kreatora wymiany urządzenia, bez potrzeby ręcznego usuwania urządzenia z systemu i dodawania nowego
- System powinien umożliwiać wykonywanie kopii zapasowych konfiguracji systemu
- System powinien umożliwiać tworzenie struktury federacyjnej w której to niezależne od siebie rozproszone systemy VMS zarządzane są z jednego centralnego miejsca.
- System powinien umożliwiać przenoszenie kamer pomiędzy rejestratorami bez utraty zapisanych zarchiwizowanych danych

System VMS Video Management Systems

Przewidziano instalację serwera VMS Video Management Systems. Serwer zaprojektowano w szafie teleinformatycznej w wydzielonym, wentylowanym, i klimatyzowanym pomieszczeniu serwerowni [1.12].

Serwer należy skonfigurować tak by obsługiwał i rejestrował obraz z lokalnych kamer zainstalowanych w projektowanym budynku, zaprojektowany VMS Video Management System ma mieć możliwość takiej rekonfiguracji by było możliwe wyświetlanie obrazu z kamer zainstalowanych w budynkach:

- Centrum Symulacji Medycznej przy ul. Sebastiana Klonowica 50
- Międzywydziałowym Centrum Dydaktyki nr 3 przy pl. Polskiego Czerwonego Krzyża 1

Przewidziano upgrade VMS Video Management System na okres 3 lat dla nowoprojektowanego systemu.

Serwer spełniający wymogi dla projektowanego docelowego systemu powinien spełniać następujące wymagania:

- Obudowa rack 2U
- Kieszenie dla 8 dysków HDD,
- Konfiguracja RAID-6
- System operacyjny Win 11 Pro 64-bit
- Pamięć RAM min.16GB

- procesor serii Intel XENON E2300 lub równoważny
- karta sieciowa 2x 1Gb
- dysk SSD (SATA III min.64GB)
- zasilanie 230V / 800W redundantne
- temperatura pracy 5°C - 40°C

Dla ilości kamer przedstawionych na rzutach i schemacie, w celu nagrywania i archiwizowania obrazu w czasie 30 dni należy zapewnić poniższe przestrzenie dyskowe:

HDD K3 + LPR 2,3TB 23,8 Mbit/s

Ilość	Rozdzielczość	Codec	klatek na sekundę	Storage duration / Activity / Motion	Storage	Bandwidth
x25	2560x1920	H.265	6fps, 710kbit/s	30d 24h 30% motion	1,7 TB	17.8 Mbit/s
x4	1920x1080	MJPEG	1fps (189kB),1,5bit/s	30d 24h 30% motion	587.9 GB	6 Mbit/s

HDD Prosektura 8,2TB 83,4 Mbit/s

Ilość	Rozdzielczość	Codec	klatek na sekundę	Storage duration / Activity / Motion	Storage	Bandwidth
x13	2560x1920	H.265	25fps, 3 Mbit/s	30d 24h 30% motion	3,7 TB	38,5 Mbit/s
x5	3840x2160	H.265	25fps, 3 Mbit/s	30d 24h 30% motion	2,4 TB	25 Mbit/s
x4	3840x2160	H.265	25fps, 3 Mbit/s	30d 24h 30% motion	2,0 TB	20 Mbit/s

6.4.6 Stacja operatora

Dla monitorowania lokalnego wybranych kamer można wykorzystać dowolny komputer wpięty w sieć z poziomu przeglądarki albo zainstalowanej aplikacji lub z dedykowanej stacji klienckiej o wyspecyfikowanych parametrach typowych lub lepszych:

- system operacyjny Win 10 Pro 64-bit
- pamięć RAM 4x4GB
- procesor serii Intel i7 – 4790 lub równoważny
- karta sieciowa 2x 1Gb
- dysk SSD (SATA III min. 64GB)
- cztery wyjścia monitorowe HDMI/ DVI / Display port

System musi zapewniać nieograniczoną licencyjnie ilość jednoczesnych połączeń klienckich z komputerów zdalnych wyposażonych w aplikacje kliencką systemu, urządzeń mobilnych obsługiwanych przez system Android lub iOS oraz z przeglądarki internetowej.

Ze względu na wrażliwe dane jakimi będą nagrania, system nie powinien umożliwiać operatorom dowolnego eksportu i kopiowania nagrań. Eksport i kopiowanie nagrań powinno być możliwe tylko w przypadkach uzasadnionych i powinno być autoryzowane przez dwóch użytkowników systemu, a mianowicie operatora i administratora (kierownika) przez tzw. Funkcjonalność dualnego logowania.

System musi zapewniać możliwość importu użytkowników do systemu z usług katalogowych systemu min. Active Directory i LDAP oraz wykorzystanie mechanizmów jednorazowego logowania do systemu tzw. SSO.

Ponadto system musi posiadać moduł umożliwiający wykonanie audytu działań operatora z poziomem szczegółowości umożliwiającym weryfikację każdego działania na interfejsie min. dokładnego momentu eksportu kamer, zakresu eksportu materiału video, wyzwolenie makr, wybór kamer do podglądu video, przełączanie widoku, wyzwolenie przekaźnika w kamerach itd. Dane o działaniach muszą być przetrzymywane w bazie danych systemu VMS z możliwością filtrowania po nazwie użytkownika, stanowiska na jakim użytkownik się logował oraz działań, które były wykonywane. Każde działanie odkładane jest jako zdarzenie na liście zdarzeń w bazie danych. Wszystkie zdarzenia mogą podlegać reakcji przez marko – np. wysłanie e-mail'a do administratora w przypadku eksportu materiału

System musi umożliwiać wyznaczenie limitu z dokładnością do godziny dostępu do materiału video dla operatora, czyli np. operator może mieć dostęp do materiału video nie starszego niż 5 godzin.

Dostosowany do użytkownika widok powinien odnosić się do graficznego interfejsu użytkownika („GUI”), który sam jest tworzony przez użytkownika lub administratora systemu. Widok operatora umożliwia mieszanie i umieszczanie dowolnej liczby i rozmiaru panelu podglądu na żywo, panelu odtwarzania, panelu alarmów i zdarzeń, panelu mapy, panelu podglądu zdarzeń na żywo, panelu zegara, licznik w ramach tego samego GUI zgodnie z wymaganiami operatora. Nie może być ograniczeń co do tego, jak użytkownik chce, aby wyglądał jego układ. Użytkownik będzie mógł zapisywać predefiniowane układy jako skróty na klawiszach funkcyjnych klawiatury od F1 do F12. Użytkownik może wykonać szybkie przełączanie układu, naciskając dowolny zaprogramowany przycisk CTRL + F1, do F12.

System powinien zapewniać elastyczność pozwalającą na wyświetlanie pojedynczego widoku lub układu widoku na wielu monitorach, aby przełączyć się na kompletny, inny układ za pomocą jednorazowej akcji, ręcznie lub automatycznie w oparciu o alarm lub zdarzenia.

Możliwość tworzenia elastycznego interfejsu użytkownika zgodnie z aktualnymi potrzebami, zapewniającą intuicyjną pracę oraz ekspresowy czas reakcji gwarantując tym samym, najwyższy poziom bezpieczeństwa. Dlatego praca operatora musi być wspierana przez następujące cechy interfejsu systemu:

- w pełni edytowalne przyciski ekranowe rozmieszczane w dowolnym miejscu poszczególnych widoków, zapewniające możliwość przełączenia pomiędzy widokami lub wyzwolenia zaawansowanych makr oferujących możliwość wielopoziomowych akcji, w tym min wysterowanie presetów kamery PTZ, aktywacja wyjścia przekaźnikowego w kamerze, nadanie uprawnień rozpoznania tablic rejestracyjnych dla danej kamery, sterowanie modułami
- aktywowanie dowolnego makra w tym presetów kamer PTZ po kliknięciu kursorem myszy na predefiniowanym transparentnym regionie obrazu na dowolnym widoku powiązanej kamery stacjonarnej,
- zaawansowane zbliżenia cyfrowe – możliwość zbliżenia cyfrowego dla wielu fragmentów z danej kamery, jednocześnie przy możliwości zachowania podglądu na całą obserwowaną przez nią scenę
- wsparcie dla kontrolera USB z joystickiem do kontrolowania funkcji PTZ ruchomych punktów kamerowych oraz możliwość kontrolowania kamer PTZ z poziomu panelu w oprogramowaniu

- obsługa cyfrowych modułów I/O aktywowanych z poziomu dedykowanych przycisków ekranowych lub automatycznie przez egzekucję reguł makr
- jednoczesny dostęp do 4 bieżących podglądów z kamer (w tym sterowanie funkcjami PTZ) z poziomu przeglądarki internetowej
- jednoczesny podgląd obrazu archiwalnego z minimum 48 kamer w jednym widoku
- jednoczesny podgląd obrazu na żywo z minimum 100 kamer na każdej zainstalowanej stacji operatorskiej
- jednoczesny podgląd na żywo nieograniczonej liczby kamer przypadku konfiguracji videowall,
- dostęp do serwerów z poziomu urządzeń mobilnych (iOS, Android) pozwalający na oglądanie bieżących widoków z kamer, sterowanie funkcjami PTZ oraz przechwytywanie zdjęć ze wskazanych momentów obserwowanego obrazu
- swobodne nadawanie przez administratora systemu hierarchicznych uprawnień każdemu operatorowi lub grupie operatorów korzystających z odpowiednich dla nich zasobów systemu, takich jak dostęp grup użytkowników do urządzeń, funkcjonalności urządzeń, widoków, reguł makr domyślnego widoku wyświetlanie
- edytowalne reguły makr budowane w oparciu o instrukcje warunkowe aktywowane krzyżowo przez wszelkie zasoby oraz funkcjonalności systemu (np. rozpoznanie tablicy rejestracyjnej z tzw. białej listy automatycznie aktywuje przełączenie widoku na ekranie monitora oraz otworzenie bramy wjazdowej do garażu)
- wsparcie min 8 monitorów o dowolnej przekątnej ekranu w ramach każdego stanowiska operatorskiego, w tym wirtualnego kontrolera z matrycą dotykową oraz klawiaturą numeryczną
- definiowanie widoków (wyświetlanie na pojedynczym monitorze) oraz multi-widoków (wyświetlanie na wielu monitorach) o różnej zawartości poszczególnych paneli (np. obraz na żywo, odtwarzanie, zegar, adres URL, lista zdarzeń, przycisk funkcyjny, mapa obiektu, sterowanie PTZ), dowolnym rozmiarze oraz położeniu w ekranie monitora
- obsługa funkcji tzw. videowall z możliwością zdalnego delegowania zawartości poszczególnych widoków, wyświetlanych na ekranach monitorów podrzędnych stacji operatorskich
- zbliżenie cyfrowe wybranego fragmentu obrazu bez utraty podglądu na pierwotny zakres obserwowanej sceny
- wybór kamery do aktualnego podglądu przez przeciągnięcie ikony kamery z mapy synoptycznej lub mapy Geo wskazującego dokładną lokalizację danej kamery w obiekcie,
- wskazanie materiału blokowanego przed nadpisaniem
- rozpoczęcie nagrywania po detekcji ruchu definiowanej dla dowolnego obszaru kamery
- możliwość doboru czasu nagrania dla każdej z kamer indywidualnie
- zmiana atrybutów zapisu przypisana do aktywnego profilu
- odtwarzanie ostatnich kilkunastu sekund nagrania, bezpośrednio z widoku kamery będącej aktualnie w trybie podglądu bieżącego obrazu, po kliknięciu prawym przyciskiem myszy

- dynamiczna zmian trybów, parametrów nagrywanie poprzez makra jako reakcja na dowolne zdefiniowane przez użytkownika zdarzenie w systemie
- zmiana parametrów nagrywania w oparciu o kalendarz tygodniowy lub roczny, dedykowane szczególnie dla wydarzeń niepowtarzalnych w terminarzu jak imprezy masowe
- eksport materiału z wielu serwerów jednocześnie do jednego pliku z materiałem archiwalnym
- eksport zdjęć z danego kadru musi umożliwiać operatorowi wskazać wycinek obrazu, który będzie eksportowany, zapis w formacie plików oraz wykonać korektę ustawień gammy, poziomu czerni i bieli
- eksport materiału video musi być możliwy do min. dwóch formatów: producenckim, zapewniającym największe bezpieczeństwo i szyfrowanie danych oraz ogólnodostępnym jak MP4 wraz metadany dotyczącymi min. analizy obrazu i wskazaniem występowania obiektów tzw. BLOB
- system musi zapewniać moduł zrzutu zdjęć z kamery we wskazane miejsce, w przypadku utraty połączenia pomiędzy serwerem a kamerą lub dezaktywacji kamery w serwerze
- wybór kamery do podglądu archiwalnego, przez przeciągnięcie ikony kamery z mapy synoptycznej
- oprogramowanie zapewnia możliwość planowania kopii zapasowych z nagraniami wideo i zdarzeniami do folderu lokalnego lub na zmapowany dysk sieciowy z możliwością automatycznego kasowania najstarszych kopii zapasowych w przypadku wyczerpania się miejsca do zapisu nowych kopii zapasowych. Moduł ten umożliwia automatyczny odroczone w czasie eksportu danych wideo z wybranej kamery lub kamer. Musi istnieć możliwość wyboru przedziału czasowego (z dokładnością do 1 sekundy) archiwizowanego/eksportowanego materiału, czasu uruchomienia automatycznej archiwizacji lub eksportu (z dokładnością do 1 sekundy), formatu eksportu (natywny lub MP4) i docelowego miejsca eksportu
- funkcjonalność zoomowalnych map umożliwiających wykorzystanie w wizualizacji obiektów map wektorowych, dzięki czemu na jednej tylko mapie wysokiej rozdzielczości można umieścić elementy znajdujące się na całym chronionym obiekcie, które będąc skrolowane będą zapewniać bardzo szybkie przejście, od podglądu ogólnego obrysu obiektu do wysokiego poziomu szczegółowości np. do poziomu danego pomieszczenia.
- programowa korekcja zniekształceń obrazu dla wszystkich obsługiwanych kamer w tym min dla kamer analogowych
- obsługa kamer 360 stopni typu rybie oko – odbywa się przez możliwość rozłożenia jednego strumienia kamery dowolnego producenta na trzy widoki w dedykowanych panelach umożliwiających: podgląd panoramiczny, sferyczny oraz podgląd na obszar wybrany przez obrót ePTZ i przez wskazanie przez operatora w podglądzie panoramicznym oraz sferycznym, przy czym obserwowany na tym panelu obraz jest zaznaczany obwódką w celu łatwej orientacji w obserwowanym materiale. Przetwarzanie kamer typu rybie oko musi być potwierdzone odpowiednim certyfikatem (np. Immervision Enables® lub równoważnym)

- możliwość precyzyjnej lokalizacji zdarzenia na skorelowanej mapie synoptycznej np. poprzez wskazanie przez podświetlenie transparentnych wielopolygonowych obszarów, wizualizujących miejsce wykrycia alarmu.
- możliwość korelacji dowolnej reakcji systemu np. przełączenie trybu nagrywania, wyzwolenie presetów kamery, przesłanie sygnału do systemu integrowanego, aktywacja analizy obrazu dla wybranej kamery lub grupy kamer, wyzwolenie poprzez transparentny wielopolygonowy obszar
- system ma dawać możliwość automatycznego wskazania obrazu z kamer obserwujących dany interesujący obszar obiektu bez konieczności znajomości przez operatora nazw, grupy kamer oraz ich hierarchii – funkcjonalność ta zwiększa ergonomię i szybkość pracy operatora.
- możliwość wysłania emaila z dołączanym zdjęciem prezentującym zdarzenie alarmowe, poprzez wykorzystanie silnika makr wraz z możliwością tworzenia generycznych makr – przechwytywanie wielu zdarzeń przez jedno generyczne makro
- alarmowanie o opóźnieniach w transmisji materiału z kamer – jest kluczowe w systemach wykorzystujących punkty kamerowe do: sterowania automatyką/weryfikacji procesów technologicznych, obsługi systemów rozproszonych. System musi alarmować operatora w przypadku wystąpienia opóźnień w transmisji obrazu powyżej 500 ms. System musi zapewniać operatorowi jasny komunikat np. czerwony krzyż oraz możliwość obsłużenia zdarzenia poprzez silnik makr
- komentarze operatora (bookmark) - w przypadku wystąpienia sytuacji alarmowej np. wykrycie intruza przez analizę obrazu na kamerach termowizyjnych, realizujących wirtualną ochronę obwodową, system wygeneruje u operatora automatycznie widok, gdzie operator będzie musiał wpisać odpowiednią notatkę dotyczącą zdarzenia z możliwością wskazania, aby materiał ten został zablokowany przed nadpisaniem. Administrator lub operator nadrzędny będzie miał możliwość bardzo szybkiego wyszukania zabezpieczonego zdarzenia, przez wyszukanie odpowiednich fraz komentarza, w bazie danych systemu CCTV lub przez wyszukanie komentarza na linii czasu odtwarzania materiału video czy liście zdarzeń systemu pojawiającej się w interfejsie. Dodatkowo operator ma również możliwość dodawania swoich komentarzy i wskazania materiału do zablokowania przez nadpisaniem, dla dowolnego wydarzenia wskazanego przez niego ręcznie na linii czasu odtwarzania materiału lub dla kamery z podglądem na żywo, przez wskazanie kamery i wciśnięcie przycisku generującego makro wyświetlające widok dodawania komentarza
- linia odtwarzania materiału video zapewnia operatorowi możliwość szybkiego wyszukiwania zdarzeń, dzięki podglądowi miniatur zdjęć ostatnich klatek w przód oraz w tył, w stosunku do wskazanego momentu na linii czasu, wskazanie graficznie ilości ruchu oraz graficzną reprezentację występujących zdarzeń wygenerowanych przez wejścia audio kamer, rozłączenie, połączenie kamer, analizy tablic rejestracyjnych, detekcji koloru, zakładek z komentarzem operatora oraz innych zdarzeń występujących w systemie VMS za pomocą prążków, po najechnięciu na który pojawia się zdjęcie z momentu wystąpienia zdarzenia wraz z opisem danego zdarzenia, np. nr rozpoznanej tablicy,

opis wykrycia itp.

- interfejs operatora musi zapewniać możliwość tworzenia makr wywoływanych za pomocą przycisków w widokach, które umożliwiają zmiany wszystkich dostępnych parametrów urządzeń za pomocą HTTP/API dowolnych urządzeń min. zmiana adresu IP kamery, włączenie/wyłączenie analizy obrazu wbudowanej w kamerze, włączenie/wyłączenie funkcji WDR, HLC, masek prywatności, reset urządzenia, wyzwolenie przekaźnika w kamerze, interkomie, module wejść/wyjść, za zbrojenie stref SSWiN, KD w systemach trzecich np. kontrola interkomów SIP, sterowanie automatyką w sieci IP i wiele innych. Funkcjonalność ta musi zapewniać możliwość komunikowania się z urządzeniami za pomocą metod GET, PUT, POST itp. z autoryzacją lub bez.
- możliwość wskazania priorytetów zdarzeń przez wskazanie dla każdego z typu zdarzeń (detekcja ruchu, sabotaż, LPR, detekcja twarzy itd.) indywidualnego koloru z palety minimum 255 kolorów, które są przypisane do wystąpienia zdarzeń na liście zdarzeń oraz linii czasu. Szablony kolorów muszą być możliwe do przypisania do wybranej grupy operatorów. Funkcjonalność zapewnia wysoką ergonomię pracy oraz bardzo szybką możliwość orientacji sytuacyjnej.
- możliwość nakładania masek prywatności na kamerze z poziomu interfejsu graficznego VMS. Minimum 8 masek ze wskazaniem jej wielkości, miejsca w scenie oraz indywidualnego nazwania każdej z masek

6.5 Wytyczne montażowe

- Urządzenia systemu włączane do gniazd sieci ethernet,
- Instalacja ochronnika przeciwprzepięciowego powyżej sufitu podwieszanego w obudowie izolacyjnej PCV,
- Regulacja wielkości dozorowanych scen w ramach możliwości regulacji obiektów zoom,
- Ochrona przed porażeniem - Jako ochronę przed porażeniem zastosowano samoczynne odłączenie zasilania. Wszystkie metalowe części obudów, należy połączyć skutecznie z szyną ochronną PE. Po wykonaniu instalacji zasilającej należy wykonać pomiary rezystancji izolacji kabla zasilającego oraz pomiar ochrony przeciwporażeniowej skuteczności szybkiego wyłączania.

6.6 Zasilanie systemu monitoringu wizyjnego

- Zasilanie kamer z przełączników sieciowych PoE
- Przełączniki sieciowe zainstalowane w szafach teletechnicznych będą zasilane z zasilacza za pośrednictwem listwy zasilającej.
- Zasilanie 230V poprzez centralny UPS, zgodnie z projektem instalacji elektrycznej

7 Instalacja systemu zarządzania bezpieczeństwem - SMS

7.1 Uwarunkowania wstępne projektowanego systemu

Uwzględniając politykę bezpieczeństwa Pomorskiego Uniwersytetu Medycznego system SMS ma za zadanie zarządzać, sterować, optymalizować

działania, w szczególności następujących systemów:

- system kontroli dostępu (KD)
- system dozorowej telewizji przemysłowej (CCTV)
- system wykrywania i sygnalizacji włamania (SSWiN)
- system wykrywania i sygnalizacji pożaru (SAP)
- system wideodomofonowy (interkomowy)

Do najważniejszych funkcjonalności realizowanych przez platformę SMS można zaliczyć:

- zarządzanie elementami sprzętowymi i logicznymi poszczególnych podsystemów;
- konfiguracja parametrów urządzeń KD z poziomu SMS
- wizualizacji stanu elementów sprzętowych i logicznymi wybranymi częściami podsystemów
- korelacja zdarzeń występujących w kilku podsystemach w oparciu o funkcje logiczne;
- jedna baza danych użytkowników KD, operatorów SMS i zdarzeń dla wybranych podsystemów.

Platforma zarządzania SMS musi umożliwiać wzajemne współdziałanie poniższych podsystemów za pomocą interfejsów programowych:

- Kontroli Dostępu,
- Sygnalizacji Włamania i Napadu
- Monitoringu Wizyjnego CCTV IP
- Interkomowego

Dodatkowo system SMS musi mieć możliwość integracji systemów zewnętrznych m.in.:

- Windowego
- Sygnalizacji Pożarowej
- iSRS (System Zarządzania Sal)
- ProAkademia

System Zarządzania Bezpieczeństwem (SMS) powinien być oparty o strukturę sieci IP z centralnym serwerem SMS oraz rozproszoną strukturą sterowników IP SKD, wykorzystującą standardowe łącza okablowania strukturalnego, zarówno miedzianego jak i światłowodowego. Taka konfiguracja daje możliwość łatwej i bezproblemowej rozbudowy, bez ingerencji w resztę pracującego systemu. Każdy sterownik TCP/IP systemu KD musi posiadać możliwość nadzorowania prawidłowego działania za pomocą sieci LAN i musi działać w trybie Plug-Play, wymiana uszkodzonego kontrolera powoduje pobranie automatycznej konfiguracji z serwera.

Aplikacja kliencka SMS musi być oparta na technologii Web i umożliwiać dostęp użytkownikom do interfejsu systemu za pomocą przeglądarek internetowych Internet Explorer, Chrome lub Firefox z dowolnej stacji operatorskiej podłączonej do sieci bezpieczeństwa (lokalnie lub zdalnie, np. za pomocą wirtualnej sieci lokalnej VPN). Ze względu na kwestie bezpieczeństwa, dostęp nie może wymagać instalacji jakiegokolwiek oprogramowania lokalnie na stacji operatorskiej. Musi działać zarówno w środowisku Linux, jak i Windows bez żadnych ograniczeń funkcjonalnych.

Platforma SMS musi dać możliwość diagnostyki zdalnej (przez sieć Internet) i lokalnej przez komputer w sieci, lub komputer podłączony do sterownika systemu KD z hiperterminalem.

Nienależnie informacja o błędach w komunikacji jest także odzwierciedlana diodami sygnalizacyjnymi w sterowniku lokalnym SKD.

Aby zabezpieczyć bezproblemowe działanie systemu, na wypadek braku komunikacji lub uszkodzenia serwera inteligencja musi zostać rozproszona do poziomu lokalnych sterowników SKD. Sterowniki KD muszą być wyposażone w moduły pamięci pozwalające na buforowanie transakcji w przypadku braku komunikacji z serwerem centralnym. Dodatkowo muszą przechowywać informację na temat uprawnień poszczególnych użytkowników, dzięki czemu mogą sterować elementami wykonawczymi (np. czytnikami) całkowicie samodzielnie. W momencie, gdy sterowniki KD ponownie otrzymają połączenie z serwerem, muszą zsynchronizować swoją bazę danych lokalną z serwerem centralnym (przesłanie buforowanych zdarzeń, aktualizacja uprawnień).

Dane przesyłane w systemach zabezpieczeń są kluczowe dla zachowania bezpieczeństwa. Z tego względu system SMS musi wykorzystywać najwyższej klasy protokoły kryptograficzne. Komunikacja między serwerem a stacją roboczą (stanowisko wizualizacji, punkt zdalnego zarządzania, terminal modyfikacji parametrów) musi się odbywać przez sieć TCP/IP z wykorzystaniem protokołu SSL, ze 128-bitowym kluczem.

Platforma SMS musi dawać możliwość kontroli zdarzeń, przez listę zdarzeń. Zdarzenia muszą mieć przypisany stopień priorytetyzacji oraz muszą być wyświetlane w kolorze wskazującym ich charakter (np. zdarzenia alarmowe – kolor czerwony). Lista zdarzeń może być filtrowana i w konsekwencji wyświetlane będą tylko zdarzenia określonego rodzaju. Pozwala to operatorowi wyświetlać wyłącznie wybrany typ zdarzeń. Platforma SMS musi mieć również możliwość zapisywania w systemie wszystkich ruchów wykonanych w systemie przez operatora w trakcie jego pracy na stacji operatorskiej.

System musi wyświetlać odpowiednie widoki oraz scenariusze w kilku lokalizacjach na obiekcie.

System SMS działać ma w przyszłości w środowisku wirtualnym. Wymaga się zatem aby system SMS miał możliwość pracy na m.in. w środowisku VMware. W celu zwiększenia bezpieczeństwa system w przyszłości powinien składać się z dwóch fizycznych serwerów, na których zostanie zaimplementowane środowisko wirtualne. System będzie realizował funkcjonalność „Warm stand-by-serwer” gdzie na bieżąco system SMS podstawowego serwera realizuje back-up systemu i przesyła go do serwera redundantnego.

Platforma SMS musi również umożliwiać definiowanie jakie rodzaje alarmu mają trafiać do konkretnego operatora, przykładowo pracownik ochrony ma otrzymywać zdarzenia alarmowe, pracownik administracyjny – zdarzenia związane z przemieszczaniem się pracowników, a administrator tylko zdarzenia techniczne związane z pracą urządzeń.

Dodatkowo można ustalać sekwencje zdarzeń dla różnych operatorów (np. jeden dozorca zajmuje się alarmami z jednej części budynku, a po odpowiednio długim czasie zwłoki może także obsługiwać alarmy przekierowane z innej części budynku, inny użytkownik otrzymuje alarmy wyłącznie techniczne).

Platforma SMS musi umożliwiać pełne raportowanie i archiwizację danych. System musi mieć wbudowane predefiniowane raporty, m.in:

- Raport zdarzeń i częstotliwości występowania zdarzeń;
- Raport listy użytkowników z danymi osobowymi;

- Raport obecności dla danego użytkownika i dla danego obszaru;
- Raport praw dostępu dla użytkownika i czytnika;
- Raport ścieżki użycia karty na obiekcie;
- Raport stanu sterowników i podłączonych do nich urządzeń;
- Raport stanu błędów występujących w systemie.

Dodatkowo system musi umożliwiać przygotowanie dowolnych raportów według wymogów użytkownika, przez definiowanie jaki typ danych ma znajdować się w konkretnej kolumnie raportu. System musi umożliwiać eksport raportów do plików PDF, XML, CSV.

W momencie wystąpienia zdarzenia alarmowego z każdego z podsystemów, platforma SMS musi wyświetlić dodatkowe okno alarmowe, zastępując jednocześnie wszystkie inne okna wyświetlone na stacji operatorskiej. System musi umożliwiać priorytetyzację alarmów i przypisanie ich do jednej co najmniej 20 poziomów. Okno alarmów musi prezentować listę kroków, które operator musi wykonać. Każdy krok działania może mieć charakter informacyjny (np. „Zadzwoń na policję”), jak również aktywny, który zmienia stan urządzenia (np. otwarcie drzwi). Dodatkowo musi być prezentowana operatorowi mapa synoptyczna z zaznaczonym elementem systemu, który wywołał alarm. Jeżeli do danego elementu systemu jest przyporządkowana kamera, automatycznie musi być prezentowany również obraz z danej kamery.

Aby zapewnić pełne bezpieczeństwo platforma SMS musi wykorzystywać serwery w których występuje redundancja podzespołów, m.in. zasilacza i dysków (wymagany RAID).

Zarządzanie uprawnieniami i personalizacja stanowiska pracy musi być przypisywana poszczególnym profilom użytkownika. Musi istnieć możliwość przypisywania dostępu do poszczególnych modułów poszczególnym operatorom w zależności od ich uprawnień. Po wprowadzeniu zmian konfiguracyjnych system nie może wymagać resetowania poszczególnych jednostek, wystarczające jest zapisanie zmian na serwerze głównym.

Kluczowy z punktu widzenia bezpieczeństwa i samej obsługi systemu jest interfejs użytkownika. Platforma musi oferować czytelny i intuicyjny interfejs użytkownika GUI znany wszystkim użytkownikom Internetu i Eksploratora Windows. W ustawieniach parametrów systemowych, każdy moduł obsługi poszczególnych systemów (kontroli dostępu, SSWiN itp.) musi mieć odmienny kolor tła, co podpowiada jednoznacznie użytkownikowi, w której części menu się znajduje.

System musi umożliwiać przypisanie w bazie danych do użytkownika następujących danych:

- imienia i nazwiska
- numeru karty dostępowej
- sklasyfikowania do grupy użytkowników – np. pracownik, serwisant, gość, dział kadr,
- bloku parkingowego
- samochodu
- numerów rejestracyjnych pojazdu
- telefonu
- adresu

Dodatkowo istnieje możliwość zdefiniowania dowolnych pól

dodatkowych, których wymaga inwestor. Każdy z użytkowników po zalogowaniu się do systemu może korzystać z okienek w wybranym języku: niemiecki, angielski, polski. Interfejs językowy przypisany jest do użytkownika, a nie do urządzenia. Hasło dostępowe do systemu ma składać się przynajmniej z 6 znaków, z których przynajmniej jeden to cyfra a inny to wielka litera.

System musi mieć wbudowaną mapę synoptyczną (wizualizację) za pomocą, której będzie istnieć możliwość pełnej wizualizacji stanu i zarządzania wszystkimi podsystemami. Funkcje, które muszą być realizowane przez system wizualizacji:

- System Kontroli dostępu – wizualizacja stanów czytnika, kontaktronu, elektrorygla, przycisku ewakuacyjnego i wszystkich elementów dodatkowych. Po kliknięciu ikony czytnika powinna zostać wyjustowana lista wyboru trybów pracy czytnika (m.in. stan otwarty, stan normalny, stan z potwierdzeniem operatora).
- System Sygnalizacji Włamania i Napadu – wizualizacja stanów poszczególnych elementów detekcyjnych (np. czujek ruchu PIR, inercyjnych, kontaktronowych). Zazbrajanie i rozbrajanie poszczególnych stref SSWiN.
- System Monitoringu wizyjnego – kliknięcie ikony kamery ma spowodować wyświetlenie obrazu z danej kamery. Dla kamer PTZ, pełna możliwość sterowania kamerą z poziomu mapy synoptycznej. Możliwość umiejscowienia na mapie synoptycznej przycisków, wymuszających obrót kamery PTZ w konkretne miejsce.
- System Interkomowy – kliknięcie ikony interkomu IP ma skutkować wywołaniem połączenia z danym interkomem oraz prezentację obrazu z kamery skierowanej na interkom.

System musi mieć także możliwość wizualizacji systemów zewnętrznych

min:

- System sygnalizacji zagrożenia pożarem - wizualizacja na mapie synoptycznej stanu poszczególnych detektorów i/lub stref SSP.
- System zarządzania kluczami – wizualizacja dostępności poszczególnych kluczy w depozytorze kluczy.
- System wizualizacji czujników środowiskowych

Dodatkowo mapa synoptyczna musi wspierać system widgetów, który umożliwia umieszczenie na niej dowolnych elementów, m.in.:

- Listę osób znajdujących się w danym pomieszczeniu (przy kontroli dwustronnej);
- Wykresy zawierające liczby osób przechodzących przez dane przejście;
- Listę stref SSWiN z informacją o ich stanie, umożliwiającą zazbrajanie i rozbrajanie poszczególnych stref;
- Skrót do konkretnych pozycji w menu, szczególnie często używanych przez operatora;
- Listę urządzeń z informacją o ich stanie połączenia z serwerem.

Kliknięcie każdej z ikon urządzenia prawym przyciskiem myszy, ma spowodować wyświetlanie wszystkich zdarzeń związanych z danym urządzeniem. Umożliwia to szybkie odwołanie do zdarzeń w obrębie każdego z systemów. Dodatkowo musi istnieć możliwość umiejscowienia bezpośrednio na mapie synoptycznej odnośnika do innej mapy synoptycznej (innego piętra budynku).

Projektowana platforma SMS musi realizować następujące funkcjonalności międzysystemowe, określone w opisach podsystemów:

Podsystem SSWiN i Kontroli dostępu:

- Zarządzanie systemami kontroli dostępu i SSWiN z poziomu jednego urządzenia – czytnika kontroli dostępu (m.in. zazbrajanie i rozbrajanie stref SSWiN).
- Wykorzystanie automatycznych funkcji zliczania osób wchodzących i wychodzących w obrębie stref kontroli dostępu po których strefa SSWiN zmieni swój stan oraz wykorzystanie zazbrajania czasowego;

Podsystem monitoringu wizyjnego:

- Wywołanie okna widoku kamery CCTV w sytuacjach alarmowych wywołanych przez system KD lub SSWiN (obraz wideo wspiera procesy decyzyjne w systemie) w platformie SMS.
- Rozpoczęcie zapisu materiału wideo z kamer systemu CCTV, w momencie wystąpienia określonych zdarzeń w pozostałych systemach (KD, SSWiN, SSP, Interkomowym). Zapisany materiał jest przypisany do konkretnego zdarzenia.
- Integrację funkcji analitycznych rozpoznawania numerów rejestracyjnych aut realizowaną przez system CCTV. Numer rejestracyjny pełni rolę karty dostępowej w systemie kontroli dostępu.
- Przesłanie informacji o przekroczeniu wirtualnej linii i detekcji ruchu do systemu SMS oraz rozpoczęcie określonej procedury alarmowej.
- Prezentację bezpośrednio na mapie synoptycznej obrazu z kamer. Dodatkowo możliwość wysterowania kamer PTZ oraz realizację „Presetu” bezpośrednio z mapy synoptycznej.
- Prezentacja informacji o wideointerkomach bezpośrednio w platformie SMS. Prezentowane są informacje o statusie każdego z wideointerkomów (prowadzi rozmowę, oczekuje itp.).

Podsystem Interkomowy

- Wywoływanie połączenia wideointerkomowego z poziomu mapy synoptycznej oraz prezentacja obrazu z kamery, przypisanej do danego interkomu. Dodatkowo w momencie wystąpienia połączenia przychodzącego, operator widzi na mapie synoptycznej z jakiego interkomu nawiązywana jest rozmowa.
- Generowanie automatycznych komunikatów głosowych z systemu wideointerkomowego, w sytuacjach zagrożenia (komunikaty generowane automatycznie, w określonych sytuacjach oraz uruchamiane ręcznie przez osoby nadzorujące system).
- Automatyczne rozpoczęcie rozmowy wideointerkomowej w momencie wystąpienia odpowiednich zdarzeń w pozostałych systemach.

Podsystem Sygnalizacji zagrożenia Pożarem

- Przesyłanie informacji o zdarzeniach alarmowych z centrali SSP do systemu SMS i rozróżnienie rodzaju alarmu, np. alarm pożarowy czujki, alarm pożarowy strefy, alarm tampera, brak połączenia między centralą a serwerem itp.

- definiowanie dowolnych procedur działania alarmowego w platformie SMS i kroków, które operator systemu musi wykonać (np. wywołanie komunikatu z systemu interkomowego itp.).
- wizualizacja na mapie synoptycznej stanu poszczególnych detektorów i/lub stref SSP; prezentacja stanu stref może być przedstawiona jako dynamiczna ikona umieszczona w danym pomieszczeniu lub jako pozycja w tabeli na dedykowanej mapie synoptycznej.
- należy zapewnić dwustronną komunikację z centrali SSP do systemu SMS poprzez certyfikowane połączenie

Podsystem Zarządzania kluczami

W obecnym opracowaniu nie przewidziano instalacji Podsystemu Zarządzania Kluczami, jednakże biorąc pod uwagę Wieloletnią Koncepcję Rozwoju Systemów Bezpieczeństwa na PUM projektowany system bezpieczeństwa musi umożliwiać taką instalację, integrację oraz współpracę w przyszłości. Dlatego system bezpieczeństwa musi się cechować następującymi możliwościami:

- Integracja umożliwia przesyłanie informacji między depozytorami i platformą SMS w czasie rzeczywistym.
- Wizualizację stanu depozytora i kluczy na mapie synoptycznej. Statusy obiektów reprezentowane są za pomocą dowolnie skonfigurowanych ikon.
- Wyświetlanie informacji o zdarzeniach dotyczących depozytorów oraz kluczy.
- Konfiguracja zdarzeń w systemie SMS w odpowiedzi na pojawienie się określonego zdarzenia, np. wyzwolenie widoku kamery CCTV ; stworzenie procedur postępowania, które musi zrealizować operator na wypadek zdarzenia.
- Tworzenie użytkowników w bazie danych depozytora z poziomu systemu SMS
- Synchronizacja danych użytkowników między systemami.
- Nadanie uprawnień do danych kluczy depozytora z poziomu systemu SMS. Następnie automatyczne wysłanie do depozytora
- Integracja umożliwia przełączenie się aplikacji integrującej na serwer redundantny SMS w trybie hot standby oraz cold standby

Elementami wykonawczymi platformy SMS muszą być:

- inteligentne sterowniki sieciowe pozwalające na podłączenie elementów wykonawczych systemów Kontroli Dostępu, SSWiN,
- komunikacja sieciowa
- serwer (rozbudowa istniejącego o niezbędne licencje)

Dodatkowo platforma SMS musi mieć możliwość integracji innych zewnętrznych systemów w oparciu o protokoły JDBC, XML SQL, LDAP.

Komunikacja między serwerem centralnym a serwerem monitoringu wizyjnego CCTV IP musi się odbywać w oparciu o protokół komunikacji http lub https over IP. Wymagane jest połączenie logiczne serwera centralnego i serwera CCTV w sieci TCP/IP. Przesyłane dane muszą być szyfrowane za pomocą standardu AES-CBC (256 bit). Dla każdej sesji musi być generowany

nowy klucz, aby zapobiec powtórzeniu kluczy. Klucze muszą być zapisane w pliku XML, który musi być zabezpieczony za pomocą szyfrowania AES-256. Aby zapewnić bezproblemową transmisję danych każda wiadomość przesyłana między serwerem a kontrolerem musi być poprzedzona 8-bajtowym nagłówkiem. Nagłówek musi zawierać 32 bitowe pole flag oraz 32 bitowe pole CRC, wykorzystywane do weryfikowania poprawności danych.

Komunikacja między serwerem centralnym a serwerem interkomowym musi się odbywać w oparciu o protokół komunikacji interkomowej ICX over IP/RS-232 lub analogiczny oferujący co najmniej taki zakres funkcjonalności integracyjnych. Wymagane jest połączenie logiczne serwera centralnego i serwera interkomowego w sieci TCP/IP.

Komunikacja między serwerem centralnym a serwerem monitoringu wizyjnego CCTV IP musi się odbywać w oparciu o protokół komunikacji HTTP over IP. Wymagane jest połączenie logiczne serwera centralnego i serwera CCTV w sieci TCP/IP.

Komunikacja między serwerem centralnym a centralą SSWiN musi się odbywać przez sterownik sieciowy (wymagane tylko połączenie logiczne). Komunikacja odbywa się w oparciu o protokół TCP/IP.

8 Instalacja systemu kontroli dostępu – SKD

Zgodnie z opisanymi wyżej założeniami systemów bezpieczeństwa jedną z instalacji systemów zabezpieczeń technicznych będzie instalacja kontroli dostępu.

W wybranych grupach pomieszczeń przewiduje się wykonanie instalacji systemu kontroli dostępu (KD). System KD musi spełnić wymogi klasy dostępu B i klasy rozpoznania 3.

8.1 Koncepcja sterowania dostępem

Przyjęto następujące założenia, stanowiące podstawę opracowania:

- należy nadzorować wejścia do budynku,
- należy nadzorować wszystkie pomieszczenia na piętrach z wyłączeniem toalet dla studentów.

Na wytypowanych przejściach zainstalowane zostaną w zależności od potrzeb:

- zastaw urządzeń dla kontroli jednostronnej (kontroler, czytnik kart, elektrozwoja, samozamykacz, zestaw klamka – pochwyty)
- zastaw urządzeń dla kontroli dwustronnej (kontroler, dwa czytniki kart, elektrozwoja, samozamykacz, zestaw pochwyty – pochwyty, przycisk ewakuacyjny)
- zastaw urządzeń dla kontroli jednostronnej dla zdublowanych przejść (przycisk ewakuacyjny, elektrozwoja, samozamykacz, zestaw klamka-pochwyty),
- dla przejść ograniczających dostęp do wydzielonych grup pomieszczeń przewidziano system interkomów obejmujących chroniony obszar

Dobór odpowiedniego osprzętu uzależniony będzie od klasy pożarowej wyposażanych w urządzenie kontroli dostępu drzwi.

Jak wyżej sprecyzowano drzwi będą wyposażone w pochwyty od strony ograniczonego dostępu oraz klamkę od strony chronionej. Drzwi w wykonaniu

przeciwdymowym muszą posiadać odpowiedni atest, część producentów podczas procedury uzyskiwania atestu nie przewiduje możliwości montowania elektrozaczepu na zamku głównym, w takim przypadku drzwi będą wyposażone w dodatkowy zamek powyżej zamka głównego współpracujący z elektrozaczepem, skutkować to będzie ponadto koniecznością uzupełnienia instalacji KD o:

- przycisk ewakuacyjny, zwalniający drzwi od strony chronionej w przypadku zagrożenia oraz
- przycisk wyjścia włączany na linii wejść kontrolera KD, zaprogramowana jako "przycisk wyjścia"

8.2 Dobór zastosowanych rozwiązań – system SKD

Biorąc pod uwagę uniwersalność dobranego rozwiązania, zdecydowano o wyborze czytników i kart pracujących w standardzie MIFARE, co pozwoli na standaryzację systemu z innymi systemami KD Inwestora. Karty MIFARE to jeden z najbardziej popularnych bezpiecznych standardów kart zbliżeniowych, charakteryzujących się unikalnymi indywidualnymi numerami kart zapisanych w chipie karcie, ponadto karty mogą być wyposażone w pamięć przechowującą dane przydatne dla indywidualnych zastosowań wymaganych przez użytkowników.

Na karcie MIFARE przechowywane będą informacje o zapisie i sposobie odczytu karty wg. albumu legitymacji studenta / wykładowcy (numer nadawany przez administratora bądź specjalnie zaprogramowane karty pod system ProAkademia)

Wybór dostawcy systemu będzie wymagał możliwości integracji z funkcjonującym i dalej rozbudowywanym systemem centralnego zarządzania wdrażanym w istniejących i realizowanych w obiektach PUM.

8.2.1 Czytnik zbliżeniowy

Parametry czytnika zbliżeniowego:

- Wspieranie technologii: Mifare Classic, Mifare DESFire 0.6, EV1 i EV2,
- Montaż natynkowy,
- Wszystkie elementy elektroniczne czytnika wewnątrz obudowy zalane żywicą epoksydową,
- Temperatura pracy -40°C...+65°C,
- Stopień ochrony IP54

8.2.2 Kontroler KD

Czytniki kart zbliżeniowych dla podwyższenia bezpieczeństwa systemu współpracują z niezależnymi kontrolerami, sterującymi elementami wykonawczymi (rygle, elektrozwoje, zamki elektryczne), umieszczonymi poza zasięgiem potencjalnych intruzów. W zależności od potrzeb, kontroler drzwiowy musi działać zarówno w topologii gwiazdy, jak i magistrali w zależności od stosowanego typu sterownika sieciowego. Musi istnieć możliwość stosowania obu topologii jednocześnie w ramach pojedynczej instalacji, dzięki czemu istnieje możliwość dostosowania sposobu instalacji do wymogów poszczególnych pomieszczeń:

- Obsługa minimum 2 czytników
- Minimum dwa wyjścia przekątnikowe – możliwość nadzoru 2 przejść z

- kontrolą jednostronną,
- Obsługa mierników temperatury i wilgotności
- Funkcja autotestu, pozwalająca na monitorowanie wewnętrznej temperatury, parametrów zasilania kontrolera i czytników, Stan urządzenia powinien być sygnalizowany wielokolorową diodą oraz przesyłany do oprogramowania zarządzającego w czasie rzeczywistym
- Protokół komunikacyjny czytników – Wiegand / clock&data,
- Zasilanie 12V...24V DC
- Włączenie do sieci ethernet za pośrednictwem sterownika sieciowego nadzorującego grupę kontrolerów KD
- Temperatura pracy -35°C...+65°C,

8.2.3 Sterownik sieciowy KD

Elementami wykonawczymi systemu kontroli dostępu muszą być inteligentne sterowniki sieciowe pozwalające na podłączenie kontrolerów drzwiowych. Sterownik musi komunikować się z serwerem za pomocą standardu TCP/IP. W przypadku zerwania łączności kontrolera sieciowego z serwerem, musi on nadal zarządzać elementami do niego podłączonymi. Dodatkowo musi zarejestrować w pamięci, co najmniej 5000 zdarzeń. Po ponownym podłączeniu go do serwera musi nastąpić automatyczna, wzajemna synchronizacja.

Sterownik sieciowy musi umożliwiać bezpośrednie podłączenie 4 kontrolerów drzwiowych w obrębie jednego zestawu z zasilaczem. Do każdego z podłączonych w ten sposób kontrolerów drzwiowych można podłączyć bezpośrednio czytniki oraz / lub wyprowadzić maksymalnie 4 magistrale RS485 do podłączenia kolejnych, w sumie 32 kontrolerów drzwiowych. Jeden sterownik sieciowy musi obsłużyć do 32 czytników kontroli dostępu za pomocą podłączonych kontrolerów drzwiowych.

Sterownik sieciowy musi umożliwiać podłączenie kontrolerów drzwiowych w gwiazdę, lub magistralę oraz użycie interfejsów RS232, RS485, Clock/Data, Wiegand. Sterownik sieciowy powinien spełniać poniższe wymagania:

- Szyfrowana komunikacja AES256 między sterownikiem sieciowym a serwerem SMS
- Stabilny system operacyjny,
- Możliwość podłączenie do 4 kontrolerów drzwiowych w trybie End To End Security (szyfrowanie od karty do serwera) - rozwiązanie zapewniające najwyższy poziom bezpieczeństwa poprzez możliwość szyfrowania od karty do serwera metodą AES.
- Obsługa wielu interfejsów i topologii: Wiegand, RS232, RS485, Clock/Data, TCP/IP, gwiazda i magistrala
- Ethernet Gigabit RJ-45
- Montaż na szynę DIN 35 mm
- Niski pobór mocy (ok. 2.5W)
- Zasilanie 12 – 24 V DC
- Temperatura pracy od -10 do + 60°C

8.2.4 Przycisk wyjścia

Przycisk umożliwiający wyjście z pomieszczenia z jednostronną kontrolą

dostępu przy zastosowaniu elektrozwoy lub elektrozaczepu instalowanego w drzwiach pożarowych (montaż z dodatkowym przeciwzamkiem).

- Zestyki NC/NO,
- Obciążalność 2A/30Vdc
- Montaż natynkowy i podtynkowy,
- Temperatura pracy -10°C ...+55°C,

8.2.5 Przycisk ewakuacyjny

Przycisk ewakuacyjny (zbij szybkę) w kolorze zielonym odcinający zasilanie od rewersyjnych elementów wykonawczych, umożliwiający wyjście z chronionego pomieszczenia w przypadku zagrożenia, paniki lub uszkodzenia systemu.

- Zestyki NC/NO – 2 pary styków,
- Obciążalność 2A/30Vdc
- Montaż natynkowy i podtynkowy,
- Temperatura pracy -30°C ...+55°C,

8.2.6 Czujniki kontaktronowe

- Czujniki otwarcia drzwi osiowe, dostarczane łącznie z kompletną stolarką.
- Czujnik spełniający normę EN50131-2-6 Grade 3
- Czujnik osiowy,
- Wyposażony w pętlę sabotażową
- Dostępne pierścienie dystansowe dla drzwi stalowych
- Odległość zamknięcia >15mm (nie dotyczy podłoża stalowego)
- Temperatura pracy -30°C...+60°C,

8.2.7 Elementy wykonawcze

Zamki elektryczne, zwory elektromagnetyczne, – elementy dostarczane ze stolarką drzwiową, w wykonaniu NO (rewersyjnym) z zasilaniem 12V DC.

8.2.8 Zasilacze buforowe

- Zasilacz impulsowy,
- Akumulatory rezerwowe umożliwiające d0 4h pracy awaryjnej systemu (bez zasilania podstawowego),
- Dwa wyjścia, zasilanie odbiorników i ładowanie akumulatora: 13,8V / I_{min}=4A; 13,8V/ I_{min}=1.5A
- Zabezpieczenie przeciwprzepięciowe, przeciwzwarciove, przeciwprzeciążeniowe, przeciw odwrotnym podłączeniem i rozładowaniem akumulatora,
- Sygnalizacja (wyjście przekąźnikowe) stanu zasilania podstawowego60 oraz niskiego stanu akumulatora.

8.2.9 Oprogramowanie zarządzające systemem KD

Wymaga się aby producent oprogramowania KD dostarczył oświadczenie, iż instalowana aplikacja spełnia wymagania europejskiej normy EN 60839-11-1: 2013 dotyczącej SKD na poziomie minimum GRADE 3.

- Od systemu kontroli dostępu wymaga się Neutralności maszyny

serwerowej.

- System KD musi być neutralny względem producenta maszyn serwerowych, centrali głównej tzn.
- System musi posiadać wsparcie dla serwerów fizycznych zgodnych z architekturą 64 bitową
- Producent systemu KD musi mieć możliwość dostarczenia tylko oprogramowanie i licencji

Podsystem Manager

Zaprojektowane w budynku Medycyny Sądowej PUM systemy bezpieczeństwa zostały dobrane zgodnie z wymaganiami Inwestora opisanymi w podstawie opracowania. Systemy bezpieczeństwa odpowiadają realnym i przyszłym potrzebom Inwestora w obszarze ochrony zasobów. inwestor przewiduje, możliwość przyłączenia do systemu kontroli dostępu na Pomorskim Uniwersytecie Medycznym budynków należącego organizacyjnie do innych instytucji np. do Szpitala. W takim przypadku, zakłada się, że system KD będzie pracował wg opisu ukazanego w części opisu kontroli dostępu.

W takim przypadku, Inwestor wymaga, aby zarządzanie obszarem dodawania użytkowników do systemu kontroli dostępu było możliwe bez możliwości „widoczności” innych nieistotnych dla czynności dodawania użytkowników informacji z systemu kontroli dostępu. Takie ograniczenie „widoczności” umożliwia wdrożenie aplikacji Manager.

Ponadto ze względu na wymaganą elastyczność systemu bezpieczeństwa pod kątem obsługi, zaprojektowano aplikację Manager. Aplikacja Manager powinna pozwalać na swobodne kreowanie obszaru obsługi systemów bezpieczeństwa, w szczególności nadawania uprawnień do zarządzania systemem bezpieczeństwa. Aplikacja powinna dawać możliwość w dowolnym momencie przekazanie możliwości zarządzania systemem bezpieczeństwa zarówno dla personelu ochrony jak i przeszkolonych pracowników uczelni.

Aplikacja powinna również służyć do administrowania uprawnieniami użytkowników parkingu oraz budynku. Zaprojektowano przyjazny interfejs, który pozwala administratorowi na szybkie założenie użytkownika, przypisanie kart zbliżeniowych oraz tablic rejestracyjnych z jednoczesnym zdefiniowaniem zasobów obiektu, do których dany użytkownik powinien posiadać dostęp.

Zgodność z GRADE3

Zgodnie z wymaganiem Grade 3 i 4 system musi posiadać mechanizm audytu/logowania informacji, który operator szukał, wyświetlał dane historyczne systemu KD. Dane, które mają się logować to minimum ID operatora oraz data i godzina wyszukiwania zdarzeń.

RODO i Ochrona danych osobowych

Zgodnie z RODO dane osobowe muszą być chronione przed wszelkimi przypadkami nadużycia w najlepszym możliwy sposób. Dane osobowe mogą być zapisane w bazie danych SKD, z tego powodu baza danych i kopia zapasowa bazy danych musi być zabezpieczona przed wyciekiem danych. Oprogramowanie SKD musi zapewniać odpowiednie mechanizmy zabezpieczające:

- Dane osobowe w kopii zapasowej SKD nie mogą być odczytywane przez

- osoby nieupoważnione
- Kopia bazy danych musi być zaszyfrowana
- Kopia bazy danych musi być zabezpieczona przed możliwością odczytu, importu i przywrócenia na innym serwerze SKD bez kluczy szyfrujących z serwer podstawowego
- SKD musi posiadać dziennik logów, z informacją, kto żąda kluczy szyfrujących, aby przywrócić bazę danych
- Kopia zapasowa SKD może być używana przez serwery redundantne automatycznie bez ograniczeń
- Backup techniczny – Do celów serwisowych musi istnieć możliwość utworzenia kopii zapasowej bez informacji poufnych

W kontekście RODO procesy systemowe muszą być identyfikowalne z osobą. Z tego powodu w systemie KD musi istnieć możliwość nadania praw 'super użytkownika' do każdej osoby indywidualnie, która ma posiadać uprawnienia administratora, mając prawo do tworzenia i zarządzania użytkownikami systemu. Super użytkownik musi być identyfikowany z imieniem i nazwiska a jego operacje logowane a dzienniku zdarzeń.

Prawa Dostępu

Ze względów bezpieczeństwa system KD musi umożliwiać politykę nadawania haseł do systemu. Minimalne wymagania do polityki haseł to:

- Długość hasła:
 - Minimalna długość hasła 4 znaki
 - Maksymalna długość hasła 32 znaki
- Czas ważności hasła:
 - Minimalny okres ważności hasła 30 dni
 - Maksymalny czas trwania ważności hasła 365 dni
- Hasło bez ograniczeń czasowych (hasło nigdy nie wygasa)
- Wymuszanie zmiany hasła:
 - Po minimum 7 dniach
 - Po maksimum 30 dniach
- System KD musi informować zalogowanego użytkownika o potrzebie zmiany hasła za pomocą powiadomienia wyświetlonego w oknie dialogowym
- Wybór „siły” hasła powinien narzucać do wyboru następujące scenariusze:
 - Wielka litera, mała litera, cyfra
 - Wielka litera, mała litera, znak specjalny
 - Wielka litera, mała litera, cyfra, znak specjalny
- Możliwość wprowadzenia ustawienia maksymalnej próby wprowadzenia błędnego hasła podczas logowanie z przedziału:
 - Np. 0 brak ograniczeń
 - Do 99 lub więcej prób
- Możliwość czasowego blokowania konta po przekroczeniu maksymalnej próby wprowadzenia błędnego hasła w czasie z przedziału od 1 minuty do 24 godzin
- System KD powinien logować w dzienniku zdarzeń zdarzenia związane z logowaniem się operatorów w minimalnym zakresie:
 - Użytkownik X zalogował się

- Użytkownik X wylogował się
- Logowanie użytkownika X nie powiodło się
- Logowanie użytkownika X nie powiodło się, czasowa blokada użytkownika

Funkcje Systemu

- Funkcja blokady (śluzowość)
- Możliwość tworzenia blokady przejść (śluzowości) dla minimum 32 czytników
- Śluzowość podstawowa – Minimalnym elementem monitorującym spełnienie warunków śluzowości to stan otwartości drzwi (kontaktron)
- Śluzowość rozszerzona – System musi umożliwiać skonfigurowanie funkcjonalności śluzowości rozszerzonej gdzie monitoring otwartości drzwi oprócz sygnału z kontaktronu uzupełniony jest o sygnał stanu rygla oraz stanu wykładki (zamka/cylindra). Każdy z w/w sygnałów musi posiadać w systemie osobny typ zdarzenia z możliwością raportowania. Niedopuszczalne są rozwiązania zrównoleżenia w/w sygnałów na poziomie fizycznym/sztynno-drutowym.
- Śluzowość musi być funkcjonalnością lokalną danego kontrolera IP, który zarządza sterownikami drzwiowymi
- Śluzowość musi działać niezależnie w przypadku braku połączenia z serwerem głównym
- System musi umożliwiać konfigurowanie grup śluzowości z możliwością:
- Zdalnego otwarcia przejścia przez operatora mimo niespełnienia warunków śluzowości przez wszystkie drzwi.
- Blokowanie możliwości zdalnego otwarcia przejścia przez operatora mimo niespełnienia warunków śluzowości
- Kontrolery KD muszą umożliwiać podłączenie wejścia awaryjnego/wejścia wysokiego priorytetu, który umożliwi odblokowanie drzwi mimo niespełnienia warunków śluzowości
- System KD musi umożliwiać automatyczne wylogowywanie operatora (AWO) w przypadku braku aktywności w aplikacji do zarządzania KD. Minimalne wymagania:
- Możliwość aktywacji funkcji AWO dla wszystkich lub wybranych użytkowników systemu
- Możliwość przypisania indywidualnego czasu „braku aktywności” dla każdego użytkownika/operatora podawanego w minutach
 - Minimalny czas braku aktywności to 1 minuta
 - Maksymalny czas braku aktywności operatora musi wynosić 1 rok lub więcej

Funkcje bezpieczeństwa: osoba znajduje się w strefie zbyt długo

System KD musi posiadać możliwość wykrywania, czy osoba nie znajduje się zbyt długo w danych obszarach bez wychodzenia. Jeżeli osoba znajduje się w jednym lub wielu obszarach zbyt długo, system musi umożliwić wygenerowanie zdarzeń, które mogą wywołać procedurę dla dalszych działań na tym wydarzeniu.

Funkcja może być wykorzystana np. do weryfikacji osób pracujących samodzielnie. Wymagane scenariusze konfiguracyjne i funkcjonalne:

- Ustawienie indywidualne dla każdej osoby o maksymalnym czasie przebywania we wszystkich obszarach
- Ustawienia indywidualne dla obszarów o maksymalnym czasie przebywania w danym obszarze
- Możliwość użycia obu ustawień równolegle
- Generowanie zdarzenia/eventu typu „Osoba XXX zbyt długo przebywająca w obszarze XXX” i powiadomienie operatora
- Ustawienie minimalnego czasu przybywania w obszarze dla wartości 60s
- Ustawienie maksymalnego czasu przybywania w obszarze, co najmniej 48 godzin

Moduł Gościa

System KD musi posiadać moduł Gościa (Vistor). Minimalne wymagania funkcjonalne:

- Status gościa w systemie KD to minimum: Zgłoszony, przybył, obecny
- Możliwość automatycznego poinformowania za pomocą maila „opiekuna gościa” o przybyciu gościa na obiekt w momencie:
- Zmiany status gościa z poziomu aplikacji recepcji
- Użycia karty gościa na czytniku KD

Dwustopniowe uwierzytelnianie/autoryzacja operatora.

- System KD musi umożliwiać wszystkim lub wybranym operatorom możliwość dwustopniowej weryfikacji, która ma być dodatkową warstwą bezpieczeństwa.
- Weryfikacja z dodatkową warstwą bezpieczeństwa jest potwierdzeniem, że osoby, próbujące uzyskać dostęp do konta są tym, za kogo się podają.
- Weryfikacja dwuetapowa zapewnia większe bezpieczeństwo konta operatora systemu KD, ponieważ logowanie obejmuje dwa etapy weryfikacji.
- Oprócz hasła trzeba też podać kod wygenerowany przez aplikację na telefonie.

Wymagany schemat działania weryfikacji dwustopniowej:

- Najpierw użytkownik musi wprowadzić swoją nazwę użytkownika i hasło. Następnie, zamiast natychmiastowego uzyskania dostępu do interfejsu GUI, użytkownik będzie musiał podać inną dodatkową informację (drugi czynnik)
- Druga informacja musi pochodzić z urządzenia/smartfonu operatora z funkcją uwierzytelniania np. aplikacja Google Authenticator lub równoważna
- Wartość drugiego czynnika (kilku cyfrowy numer) musi być losowy i zmieniać się, co kilkanaście, kilkadziesiąt sekund
- Smartphone musi zostać „sparowany” kontem operatora system KD

Karta dostępową

System KD musi umożliwiać następujące funkcjonalności związane z kartą dostępową:

- Czas automatycznej dezaktywacji karty – W szczegółach karty

użytkownika musi być wyświetlana ilość dni, która pozostała do automatycznej dezaktywacji kart

- Karta strażaka – Karta dostępowa musi posiadać funkcje karty strażaka. Funkcja pomaga wprowadzać ustawienia priorytetowe dostępu dla strażaków lub innych osób, które mogą być zaangażowane w sytuacje awaryjne na obiekcie.
- Aktywacja funkcji karty strażaka w systemie KD dla wybranej karty powoduje, że karta posiada najwyższy priorytet z automatycznymi ustawieniami:
 - Ważności karty: Tak
 - Okres ważności karty: bez limitu
 - Czasowy AntyPassBack: Wyłączony
 - Karta nieważna, gdy używana dłużej niż: Karta zawsze aktywna

Statusy otwarcie drzwi

- Drzwi otwarte
- Drzwi zamknięte
- Pre-Alarm drzwi otwarte zbyt długo
- Drzwi otwarte zbyt długo
- Drzwi otwarte w nieoczekiwany sposób
- Drzwi otwarte od storn niechronionej

8.2.10 Serwer systemowy

Należy doposażyć istniejący serwer o odpowiednie licencje. Administrowanie system KD może odbywać się z dedykowanej stacji klienckiej: obudowa 2U rack,

- system operacyjny Win 10 Pro 64-bit
- pamięć RAM min. 4x4GB
- procesor serii Intel i7 – 9700 lub równoważny
- karta sieciowa 2x 1Gb
- dysk SSD (SATA III min. 64GB)
- dwa wyjścia monitorowe DVI / Display port
- zasilacz 300W

Stacja robocza umożliwiająca administrowanie system KD (administrowanie, czyli nadawanie uprawnień dla nowych użytkowników oraz ewentualne generowanie wymaganych raportów) zostanie umieszczona w pomieszczenia administratora lub ochrony obiektu.

Dodatkowa funkcjonalność - System Rezerwacji Sal iSRS

Jest to rozwiązanie, które porządkuje oraz usprawnia sposób zarządzania salami dydaktycznymi. System iSRS rozszerza funkcjonalność systemu kontroli dostępu i umożliwia:

- dokonywanie rezerwacji pomieszczeń w formie kalendarza,
- automatyczne nadawanie dostępu do wybranych pomieszczeń dla wykładowców,
- wyświetlanie informacji o rezerwacjach na portalu WWW uczelni na telewizorach dla lokalizacji których w projekcie instalacji teletechnicznych przewidziani gniazda przyłączeniowe do sieci LAN.

- raportowanie zajętości sal,
- automatyczne importowanie planu zajęć, studentów i wykładowców z systemu ProAkademia,
- odsyłanie do systemu ProAkademia przydzielonych sal lekcyjnych (o ile sale te nie były przydzielone w ProAkademia),
- odsyłanie do systemu ProAkademia obecności studentów na zajęciach,
- raport z obecności studentów na zajęciach,
- monitorowanie konfliktów w przydzielaniu sal do zajęć,
- pośredniczy w komunikacji systemu kontroli dostępu z ProAkademia i umożliwia automatyczne zakładanie profesorów i studentów w systemie ProAkademia.

Istniejącą aplikację iSRS znajdującym się w Centrum Symulacji Medycznej, należy rozszerzyć o licencję do obsługi systemu rezerwacji sal iSRS dla projektowanego budynku.

Rozbudowa oprogramowania iSRS na istniejącym serwerze jest wymagana, aby utrzymywać spójny sposób synchronizacji danych dla wszystkich istniejących i nowych budynków.

Należy także przewidzieć zgodność oprogramowania iSRS z oprogramowaniem KD do wersji zgodnej z upgradowaną wersją oprogramowania serwera KD.

Podstawowa funkcjonalność – integracja z ProAkademią

W ramach budowy Międzywydziałowego Centrum Dydaktyki nr 3 zrealizowano proces automatycznego importu danych studentów z systemu ProAkademia do systemu kontroli dostępu.

Zaplanowano proces automatycznego importu danych studentów z systemu ProAkademia do systemu kontroli dostępu. Ta operacja przewiduje import danych takich jak imię, nazwisko itd. oraz numer legitymacji do systemu kontroli dostępu. Aby dokonać tego procesu przewidziano integrację z systemem ProAkademia. W związku z przewidywaną integracją przewiduje się dokonać integracji w ramach istniejącego serwera głównego zlokalizowanego w budynku MCD-3.

Przewidziano upgrade istniejącego serwera kontroli dostępu do aktualnej wersji. W chwili obecnej w Centrum Symulacji Medycznej wykorzystywane są czytniki, które odczytują nr seryjny kart Mifare, i do systemu kontroli dostępu iProtect dodane są tylko karty pracowników uczelni (wykładowców/ osób techniczno-administracyjnych). Są to numery seryjne (sektor 0) karty Mifare. W związku z powyższym, przy przejściu na współpracę z kartami systemu kontroli dostępu dla studentów, zawierających unikalny numer albumu.

W ramach integracji z ProAkademią należy zaimportować do systemu kontroli dostępu numery albumu studentów zapisane na kartach Mifare. Dzięki czemu czytniki kontroli dostępu będą odczytywały karty studenckie i identyfikowały je właśnie po tych numerach albumu. W systemie kontroli dostępu iProtect dotychczasowe dane dotyczące kart Mifare (czyli nr seryjny kart) nie będą już prawidłowo działać na tak przeprogramowanych czytnikach. W związku przewidziano dostarczenie dla wykładowców i pracowników PUM nowe karty, które będą miały zapisane dane w tym samym obszarze pamięci karty Mifare co karty studentów. Będą to dane, które nie pokrywają się z nr albumu studentów, tak aby móc odróżnić takie karty od kart studenckich.

Powyższy opis ukazuje schemat, wg którego na Międzywydziałowym Centrum Dydaktyki nr 3 oraz Centrum Symulacji Medycznych powinien działać system KD. W budynku Pomorskiego Uniwersytetu Medycznego w projektowanym Budynku Medycyny Sądowej wymagane jest identyczne programowanie czytników.

8.2.11 Karty bezstykowe autoryzacji dostępu

W systemie będą używane karty bezstykowe MIFARE.

8.2.12 Okablowanie SKD

Całość okablowania SKD przebiegającego w drogach ewakuacyjnych jak i poza nimi wykonać w klasie CPR B2 ca s1 d1 a1.

Wymogi takie spełniają między innymi przewody:

- okablowanie czytników - skrętka ekranowana typu CAT6A STP B2ca,
- okablowanie zamków elektrycznych, kontaktronów, czujników - skrętka typu HTKSH 4x2x0,8,

8.3 Bilans energetyczny SKD

Zasilanie wszystkich modułów systemowych oraz zasilaczy doprowadzić do najbliższej rozdzielni elektrycznej, w której wydzielono wydzielony obwód do zasilania systemu SKD i SWiN:

Jako zasilanie awaryjne projektowane są baterie akumulatorów instalowane w modułach wyposażonych w zasilacze zasilające urządzenia aktywne oraz wykonawcze systemu kontroli dostępu. Przełączanie na zasilanie awaryjne odbywać się będzie automatycznie po zaniku zasilania podstawowego.

Wymagana pojemność akumulatorów:

$$Q = k \times (I_1 \times t_1 + I_2 \times t_2)$$

Q – wymagana pojemność akumulatora

k- współczynnik zależny od czasu dozoru przyjęto k=1,25

I₁ – całkowity prąd dozoru

I₂ – całkowity prąd alarmowania/ sterowania

t₁ – czas dozoru – wymagany czas dozoru,

t₂ – czas alarmowania / sterowania równy 0,5h

Zgodnie z wymaganiami normatywnymi dla systemu KD Grade 2 / Grade 3 należy zapewnić odpowiednio 2h / 4h czasu podtrzymania pracy systemu bez zasilania podstawowego.

W przeprowadzonej analizie założono zasilanie z jednego zasilacza do 4 kontrolerów (maksymalnie 8 nadzorowanych przejść oraz jednego kontrolera sieciowego).

Dla zasilania grupy kontrolerów obsługujących 8 przejść przewidziano jeden zasilacz buforowy							
GRADE 3				GRADE 2			
kontroler sieciowy	0,208 A	1 szt.	0,208 A	kontroler sieciowy	0,208 A	1 szt.	0,208 A
kontroler drzwiowy	0,040 A	4 szt.	0,160 A	kontroler drzwiowy	0,040 A	4 szt.	0,160 A
czytnik kart	0,058 A	8 szt.	0,467 A	czytnik kart	0,058 A	8 szt.	0,467 A
elektrozwozowa	0,032 A	8 szt.	2,560 A	elektrozwozowa	0,032 A	8 szt.	2,560 A
akumulator 17Ah		1 szt.		akumulator 17Ah		1 szt.	
zasilacz 12V/7A		1 szt.		zasilacz 12V/7A		1 szt.	

	razem	3,395 A			razem	3,395 A
dobór wymaganego źródła zasilania awaryjnego				dobór wymaganego źródła zasilania awaryjnego		
$C_{min} = 1,25 * (A1 * t1 + A2 * t2)$				$C_{min} = 1,25 * (A1 * t1 + A2 * t2)$		
t1 (minimalny czas czuwania) =		4h		t1 (minimalny czas czuwania) =		2h
	Cmin =	18,05 Ah			Cmin =	9,56 Ah
zastosowano akumulator o pojemności	Cnom =	18,00 Ah		zastosowano akumulator o pojemności	Cnom =	12,00 Ah
przewidywany czas pracy awaryjnej	t1 =	3,99 h		przewidywany czas pracy awaryjnej	t1 =	2,57 h

8.4 Struktura sieciowa instalacji KD

Projektowany system składa się z następujących wykorzystywanych modułów, wymagających zasilania:

- Kontrolery sieciowe
- Kontrolery drzwiowe
- Czytniki bezstykowe
- Przyciski ewakuacyjne
- Przyciski wyjścia
- Elektrozwory

9 System parkingowy

9.1 Koncepcja systemu rozpoznawania tablic rejestracyjnych

System wideodetekcji numerów rejestracyjnych pozwoli na parkowanie pojazdów zapisanych w systemie.

Serwer systemu parkingowego zaprojektowano w zarezerwowanej szafie teleinformatycznej w wydzielonym, wentylowanym, i klimatyzowanym pomieszczeniu serwerowni [1.12]. Informacje będą wyświetlane w systemie PSIM.

9.1.1 Kamera LPR

Kamera dedykowana do funkcji rozpoznawania numerów rejestracyjnych pojazdów, kamera wysyła rozpoznany numer do serwera nadzorującego system KD, w przypadku zarejestrowanego numeru w bazie użytkowników uprawnionych do korzystania z parkingu otwiera odpowiedni szlaban skojarzony z kamerą.

Zaplanowano, iż administrowanie uprawnieniami użytkowników parkingu zarządzać będzie oprogramowanie systemu KD w które pozwala administratorowi na szybkie założenie użytkownika, przypisanie kart zbliżeniowych oraz tablic rejestracyjnych z jednoczesnym zdefiniowaniem zasobów obiektu, do których dany użytkownik powinien posiadać dostęp.

Kamery rozpoznające tablice rejestracyjne: muszą spełniać poniższe wymagania:

- Przetwornik czarno biały z globalną migawką (global shutter) minimum 1920 x 1080 pikseli i 60 kl./s
- Maksymalna prędkość pojazdu: 70 km/h (wersja krótka)
- Skuteczność rozpoznania tablic LPR > 95%
- Obsługa min. jednego pasa ruchu
- Zintegrowany oświetlacz IR z diodami LED @ 850 nm, stroboskop
- Gigabit Ethernet 10/100/1000
- microSD do 64 GB wewnątrz kamery (8 GB w standardzie)

- Buforowanie danych o tablicach wykonywane w pamięci kamery - po przywróceniu komunikacji danych z serwerem dane są automatycznie synchronizowane z bazą danych z okresu braku komunikacji
- Algorytm Autolris zintegrowany bezpośrednio z kamerą pozwalający na dynamiczną regulację parametrów akwizycji (wzmocnienie, czas strobo, czas migawki)
- LPR wykonywany dokładnie na bazie składni tablic danego kraju na bazie implementowanych bibliotek do wyboru minimum dla Polski i wszystkie kraje UE (na podstawie dyrektyw Ministerstw Transportu każdego kraju)
- Wskazywanie krajów pochodzenia tablic rejestracyjnych
- Odczytywanie kodów KEMLER
- Szacowanie prędkości poruszania się pojazdu na bazie analizy obrazu – zapewnienie dokładniej kalibracji przez wskazanie wysokości montażu oraz kąta nachylenia do pasa ruchu
- Kamera musi być w stanie wskazać kierunek przejazdu rozpoznanego pojazdu z wykorzystaniem analizy obrazu
- Obiektów kamery MUSI być stały– nie dopuszczalna jest zmiennoogniskowa, która w czasie poruszania się pojazdu mogłaby ulec rozmazywaniu uniemożliwiając zapewnić wysoką skuteczność
- Możliwość zarządzania dwiema listami tablic rejestracyjnych bezpośrednio w kamerze
- Możliwość odbioru ramki z zewnętrznej kamery kontekstowej IP spośród obsługiwanych przez kamerę do odczytu tablic rejestracyjnych. W przypadku każdego rozpoznania kamera do odczytu tablic rejestracyjnych zapewni:
 - Obraz czarno-biały wykonany przez kamerę do odczytu tablic rejestracyjnych
 - Obraz kontekstowy wykonany przez zewnętrzną kamerę kontekstową
- Zasilanie: 24 Vdc lub PoE +
- Zużycie: max 12 W
- Odporność na warunki środowiskowe IP67
- Zakres temperatur: -40°C / +60°C
- Odległość odczytu: min. 8 metrów
- Obsługa portu szeregowego oraz protokołu Wiegand do bezpośredniej integracji min z systemami SKD, BMS, VMS
- Protokoły: FTP, SFTP, FTPS, HTTP, HTTPS Post, JSON, XM, IEEE1588
- Szyfrowanie obrazu AES256 certyfikowane zgodnie z OIML D31 do 2030, wykonywane bezpośrednio na kamerze
- Tryby pracy:
 - dowolny ruch - ciągle przechwytywanie i przetwarzanie obrazu
 - wyzwalone: przechwytywanie i przetwarzanie obrazu wyzwalone przez Ethernet (API/SD),

9.1.2 Szlaban elektryczny

Konstrukcja szlabanu powinna być odporna na zmienne warunki atmosferyczne, bryzgoszczelna, obudowa szlabanu powinna być wykonana z

aluminium malowanego proszkowo. Ramię szlabanu powinno być wykonane z profilu aluminiowego z osłoną z pianki zabezpieczającą przed uszkodzeniem karoserii pojazdu w przypadku kolizji.

- czas otwarcia/zamknięcia maksymalnie 1,3 sekundy,
- długość ramienia 3,5 m,
- mechanizm bezolejowy,
- przekładnia wyposażona w zintegrowany czujnik przeciążeniowy,
- możliwość awaryjnego otwarcia bez użycia dodatkowych narzędzi,
- automatyczne otwarcie ramienia w przypadku zaniku zasilania nastąpi w czasie nie dłuższym niż 2 sekundy,
- szlaban ma możliwość blokowania ramienia w pozycjach krańcowych,
- szlaban wyposażony w system bezpieczeństwa powodujący automatyczną zmianę kierunku ruchu w przypadku wykrycia oporu,
- urządzenie jest wyposażone w wbudowany dwukanałowy detektor pętli indukcyjnych,
- ilość cykli szlabanu (MCBF) 10 mln ,
- maksymalny pobór mocy 100W,
- klasa szczelności IP54,
- zasilanie 230V,
- zakres temperatur pracy od – 30°C do + 55°C,
- obudowa aluminiowa ze zdejmowaną pokrywą ułatwiającą dostęp serwisowy,
- Możliwość ponownego montażu ramienia po jego zerwaniu przez pojazd bez uszkodzenia napędu

10 Instalacja systemu sygnalizacji włamania SWiN

10.1 Koncepcja systemu SWiN

Projektowana instalacja ma za zadanie ochronę wybranych typów pomieszczeń przed włamaniem lub wejściem niepożądanych osób. Ochrona pomieszczeń przed włamaniem będzie realizowana poprzez zastosowanie detektorów ruchu oraz czujników kontaktronowych w oknach i drzwiach oraz innych czujników wykrywających zagrożenia włamaniem (czujniki inercyjne) oraz zagrożenia techniczne (np. zalanie ważnych pomieszczeń)

Dobór systemu i współpracujących urządzeń będzie umożliwiać zarządzanie z poziomu:

- Mapy synoptycznej – zazbrajanie i rozbrajanie poszczególnych stref SWiN oraz wizualizacja stanów poszczególnych stref i elementów detekcyjnych nawet w momencie, gdy strefa nie jest zazbrojona.
- Czytnika kontroli dostępu – automatyczne zazbrajanie i rozbrajanie poszczególnych stref SWiN po przyłożeniu uprawnionej karty dostępowej lub w momencie, gdy wszystkie osoby wyjdą z pomieszczenia (realizowane w oparciu o czytniki kontroli dostępu). Wizualizacja stanu strefy SWiN na diodzie czytnika kontroli dostępu.
- Z uwagi na projektowane niezależne systemy SWiN oraz KD realizację wymaganej funkcji zapewni integracja obu systemów za pomocą odpowiedniego modułu oprogramowania integrującego, instalowanego na serwerze administracji systemem KD.
- Manipulatora SWiN – zazbrajanie i rozbrajanie po wpisaniu kodu autoryzacyjnego. Wizualizacja stanów poszczególnych stref.

Konfiguracja systemu zgodnie z uprawnieniami.

- Aplikacji mobilnej – zazbrajanie i rozbrajanie po wpisaniu kodu autoryzacyjnego. Wizualizacja stanów poszczególnych stref.
- Konfiguracja systemu zgodnie z uprawnieniami.

10.2 Wymagania dla projektowanego systemu SWiN

- zadaniem systemu SWiN jest ochrona wytypowanych pomieszczeń, dróg komunikacyjnych, otworów drzwiowych i okiennych na poziomach łatwego dostępu od zewnątrz budynku,
- system SWiN nadzorował będzie niektóre zdarzenia techniczne jak czujniki zalania istotnych pomieszczeń (serwerownie, itp.)
- podział na partycje (niezależnie uzbrajane) uwzględni:
- wydzielone obszary katedr i zakładów
- wejścia do budynku
- obszar garaży
- wydzielone pomieszczenia techniczne, magazynowe
- elementy systemu SWiN oraz sposób prowadzenia instalacji kablowej będzie zgodny z wymogami norm PN-EN 50131 dla systemu klasy Grade 3.

10.3 Dobór zastosowanych rozwiązań – system SWiN

10.3.1 Centrala alarmowa

Centrale przeznaczona są do stosowania w rozbudowanych systemach sygnalizacji włamania i napadu, obsługująca zarówno linie przewodowe jak i bezprzewodowe, o budowie modułowej rozproszonej. System budowany jest poprzez przyłączanie do magistral RS485 kolejnych modułów:

- rozszerzeń we/wyj
- szyfratorów systemowych
- opcjonalnie modułów komunikatorów GSM/GPRS
- opcjonalnie modułów linii bezprzewodowych

Centrala systemu umożliwia zarządzanie za pośrednictwem sieci IP, centrala na wbudowane mechanizmy integracji z systemem kontroli dostępu w celu zaprogramowania możliwości zazbrajania i rozbrajania stref podlegających ochronie za pomocą czytników kart.

Z uwagi na zakres przewidywanych stref ochrony wybrano centralę umożliwiającą późniejszą rozbudowę systemu SWiN o wymagane w kolejnych etapach rozbudowy strefy

- możliwość wydzielenie do 32 niezależnych stref ochrony,
- wielopoziomowa hierarchia kodów dostępu,
- zgodność z wymaganiami normy PN-EN 50131 Grade 3
- zazbrajania, rozbrajanie, za pomocą szyfratorów, pilotów bezprzewodowych, czytników kart, z poziomu oprogramowania zarządzającego

Zarówno centrala alarmowa jak i moduły rozszerzeń wyposażone w zasilacze (zasilane z transformatorów obniżających napięcie sieciowe do bezpiecznego) umożliwiające ładowanie baterii akumulatorów podtrzymujących funkcjonowanie systemu bez zasilania podstawowego. Baterie akumulatorów dobrane dla 72 godzi pracy awaryjnej.

Minimalna ilość obsługiwanych wyjść przez centralę za pomocą ekspanderów wejść/wyjść, modułów rozszerzeń i ewentualnych licencji:

- Bezpośrednio przez płytę główną centrali minimum 8 wyjść
- Bezpośrednio przez ekspandery wejść/wyjść minimum 8 wyjść
- Minimalnie 120 wyjść na za pomocą wszystkich ekspanderów wejść/wyjść
- Minimalnie 16 wyjść przez wszystkie interfejsy czytników kart podłączanych na magistrali RS-485
- Profile wyjściowe:
 - Centrala musi mieć możliwość przypisania wyjść do profili wyjściowych.
 - Centrala musi mieć możliwość dodania minimum 32 profile wyjściowe
 - Każdy z profili musi mieć możliwość konfiguracji indywidualnych parametrów w zależności od przeznaczenia i roli wyjść w systemie np. profil alarmowy, usterka, uzbrojenie itp.
- Konfiguracja ustawień profilu wyjściowego musi umożliwiać programowane parametry określające kategorie zdarzeń, na które wyjście lub wyjścia przypisane do profilu mają zmienić swój stan np. w przypadku wystąpienia zdarzenia alarmu włamaniowego, sabotaż detektora, sabotaż magistrali RS-485, awaria zasilania, awaria baterii, strefa gotowa do uzbrojenia itd.
- System musi umożliwiać wybór minimum 32 różnych typów zdarzeń, które można przypisać do profilu

10.3.2 Szyfrator OLED

Klawiatura OLED umożliwiającą zarządzanie systemem SSWiN. Wyświetlacz OLED szyfratora prezentuje informacje o systemie i umożliwia zarządzanie udostępnionymi strefami ochrony, wbudowane diody sygnalizują stan kilku wybranych stref oraz stan systemu (np. awarie).

Manipulator musi być zgodny z GRADE 3 według normy EN 50131-1

Manipulator musi posiadać wbudowane na 2 wejścia alarmowe, umożliwiające bezpośrednie podłączenie detektorów np. kontaktronów.

Wejścia alarmowe manipulatora:

- Muszą mieć możliwość konfiguracji jak standardowe wejścia podłączone na centralę alarmową i na moduł ekspandera wejść/wyjść
- Wejścia muszą mieć możliwość monitoringu linii za pomocą rezystancji
- Wejścia muszą umożliwiać konfiguracje z 5 stopniową parametryzacją (N.O., N.C., EOL, AM, Fault)

Manipulator musi występować wersji z wbudowanym czytnikiem zbliżeniowym i wersji bez czytnika Klawiatura musi posiadać przyciski:

- Numeryczne od 0 do 9
- 4 przyciski funkcyjne
- Przycisk funkcji potwierdzenia/akceptacji oraz przycisk cofnięcia
- Funkcje przycisków nawigacyjnych

Funkcja nawigacji

- Przyciski 2, 4, 6 i 8 muszą pełnić funkcje przycisków numerycznych i

nawigacyjnych

- Nawigacja to funkcja podpowiadania użytkownikowi, które opcje w menu są dostępne
- W przypadku możliwości poruszania się po menu np. górę i dół dany przycisk nawigacyjny musi zostać dodatkowo podświetlony na kolor zielony
- W przypadku brak możliwości nawigacji np. górę dany przycisk nawigacyjny nie może być podświetlany na kolor zielony

Wyświetlacz

- Manipulator musi być wyposażony w wyświetlacz w pracującej technologii OLED

Czujnik zbliżeniowy

- Manipulator musi być wyposażony w czujnik zbliżeniowy.
- Funkcją czujnika zbliżeniowego jest podświetlenie przycisków i wyświetlacza OLED w momencie wykrycia ruchu w pobliżu manipulatora.
- Manipulator musi umożliwiać konfigurację zakresu działania czułości czujnika zbliżeniowego (minimum 4 stany) oraz możliwość jego całkowitego wyłączenia
- Na ekranie głównym bez autoryzacji użytkownika za pomocą kodu PIN lub karty wyświetlacz musi wyświetlać min.:
 - Nazwę systemu
 - Dostępne funkcje dla 4 przycisków funkcyjnych
 - Datę i godzinę
 - Powiadomienie o dostępnych wiadomościach w systemie

10.3.3 Expander wejść/wyjść z zasilaczem

Pojedynczy expander z zasilaczem musi obsługiwać minimum 32 wejścia. Expander musi posiadać możliwość bezpośredniego podłączenia minimum 8 wejść fizyczne. Pozostałe 24 wejścia mogą być podłączone fizycznie bezpośrednio do złącz śrubowych ekspandera lub za pomocą dedykowanych płytek rozszerzających ilość złącz śrubowych pojedynczego ekspandera. Płytki rozszerzeń muszą być podłączone bezpośrednio do ekspandera jako jego rozszerzenie. Nie jest dopuszczalne stosowanie rozwiązania, gdzie dodatkowe płytki rozszerzeń podłączone są na magistrale RS-485.

Wszystkie 32 wejścia muszą być podłączone do jednej obudowy a rozwiązanie musi być zgodne z normą EN 50131-1 dla stopnia zabezpieczania minimum Grade 3

Pojedynczy expander wejść/wyjść z zasilaczem musi obsługiwać do 10 wyjść.

Expander musi posiadać bezpośrednio na płycie minimum 6 wyjść (2 wyjścia przekątnikowe, 2 wyjścia typy otwarty kolektor, 1 wyjście głośnikowe 8 Ohm, 1 wyjście napięciowe dla sygnalizatora optyczno-akustycznego) Pozostałe 4 wyjścia (4 wyjścia przekątnikowe lub 4 wyjścia typy otwarty kolektor) mogą być podłączone za pomocą płytek rozszerzeń podłączonych bezpośrednio do ekspandera.

10.3.4 Czujniki kontaktronowe

- Czujniki otwarcia drzwi lub okien osiowe, dostarczane łącznie z

- kompletna stolarka.
- Monitorowanie w odległości do 15mm (drewno)
- Wyprowadzony przewód połączeniowy,
- Obudowa cylindryczna, śrubowa, metalowa
- Temperatura pracy -30°C... +60°C
- Czujnik spełniający normę EN50131-2-6 Grade 3

10.3.5 Detektory ruchu

- Pasywna czujka podczerwieni ruchu
- Antymasking
- Zasięg do 12m
- Zaawansowana analiza sygnałów zmniejszająca wystąpienie fałszywych alarmów
- Pełna ochrona przed przeczołganiem
- Zasilanie 12V dc,
- Czujnik spełniający normę EN50131-2-6 Grade 3

10.3.6 Detektory ruchu dualny

- pasywna czujka podczerwieni ruchu PIR+MV,
- zasięg do 12m, ochrona przed przeczołganiem
- zasilanie 12V dc
- Czujnik spełniający normę EN50131-2-6 Grade 3

10.3.7 Czujnik zalania

Czujnik montowany w pomieszczeniach technicznych wykrywający pojawiającą się wodę w efekcie przepływu prądu między elektrodami umieszczonymi na posadzce.

- Zasilanie 12V dc,
- Zakres temperatur pracy -10°C...+55°C

10.3.8 Zasilanie SWiN

Jako zasilanie awaryjne projektowane są baterie akumulatorów instalowane w modułach wyposażonych w zasilacze zasilające urządzenia aktywne oraz wykonawcze systemu kontroli dostępu. Przełączanie na zasilanie awaryjne odbywać się będzie automatycznie po zaniku zasilania podstawowego.

Zgodnie z wymaganiami normatywnymi dla systemu SWiN Grade 3 należy zapewnić 72h czasu podtrzymania pracy systemu bez zasilania podstawowego.

Zgodnie z przedstawionym zestawieniem i po doborze czujników wykrywczych i modułów wejściowych systemu SWiN należy wyliczyć na podstawie parametrów elektrycznych tych urządzeń wymaganą pojemność akumulatorów. Wstępnie założono stosowanie akumulatorów 17Ah dla przyjętych do obliczeń urządzeń referencyjnych

10.4 Wytyczne montażowe

- moduły systemowe montować na ścianach pomieszczeń technicznych, gdzie przewidziano w projektach IE i TT doprowadzenia zasilania

- urządzeń KD i SWiN oraz gniazd sieci ethernet,
- instalację prowadzić na suficie w rurkach PCV oraz na korytach stalowych instalacji teletechnicznych, niezbędnie przewiercić przez podciąg wykonać techniką bezudarową - otwory ϕ 30 minimum co 15cm,
- instalację w rurkach PCV prowadzić w ciągach wielokrotnych w koordynacji z innymi instalacjami niskoprądowymi,
- pionowe odcinki instalacji wykonać podtynkowo w rurach giętkich PCV,
- stosować systemowe elementy połączeń kanałów i rur (uchwyty, złączki, kształtki zmiany kierunku trasy),
- przejścia przez ściany i stropy pomiędzy strefami pożarowymi zabezpieczyć materiałami o odpowiedniej odporności ogniowej,
- lokalizacje konsol szyfratorów strefowych skoordynować aparatami instalacji elektrycznej,
- Instalacje wykonać zgodnie z wymaganiami normy dla systemów Grade 3.
- Dla podłączania urządzeń wykrywczych zakończonych przewodem połączeniowym (czujniki kontaktronowe, itp.) stosować puszkę ze stykami sabotażowymi.
- Ochrona przejść przez ściany i stropy - wszystkie przepusty przez ściany i stropy uszczelnić atestowanymi materiałami o odpowiedniej odporności ogniowej.
- Ochrona przed porażeniem - Jako ochronę przed porażeniem zastosowano samoczynne odłączenie zasilania. Wszystkie metalowe części obudów, należy połączyć skutecznie z szyną ochronną PE. Po wykonaniu instalacji zasilającej należy wykonać pomiary rezystancji izolacji kabla zasilającego oraz pomiar ochrony przeciwporażeniowej skuteczności szybkiego wyłączenia.

11 Wymagania podstawowe integratora pożarowego (SIUP)

W celu zintegrowania systemów mających wpływ na bezpieczeństwo pożarowe obiektu w zakresie wizualizacji, sterowania i zarządzania urządzeniami przeciwpożarowymi oraz integracji innych systemów, należy zainstalować i wdrożyć System Integrujący Urządzenia Przeciw Pożarowe (SIUP), oparty o certyfikowaną centralę sterującą urządzeniami przeciwpożarowymi (Urządzenie integrujące wraz oprogramowaniem) spełniającą wymagania pkt. 12.1 załącznika do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 20 czerwca 2007 r. w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia do użytkowania (Dz. U. nr 143 poz. 1002; zm.: Dz. U. z 2010 r. nr 85, poz. 553 oraz z 2018 r. poz. 984).

Platforma informatyczna SIUP musi być oparta o oprogramowanie klasy Physical Security Information Management (PSIM).

Platforma sprzętowa SIUP musi być oparta o minimum:

- komputer przemysłowy
- przełącznik sieciowy z wbudowanymi 8 portami typu 1000Base-T oraz minimum 2 portami typu SFP
- zasilacz buforowy zintegrowany z oprogramowaniem PSIM w celu wizualizowania stanów pracy (awaria, praca na zasilaniu bateryjnym)
- wizualizację stanu pracy urządzenia znajdującą się na frontowym panelu

(zasilanie z sieci 230V, awaria zbiorcza)

- wentylator z modułem termostatu
- sygnalizację otwarcia obudowy wizualizowaną z poziomu oprogramowania PSIM w celu detekcji nieautoryzowanych ingerencji
- moduł komunikacyjny zawierający minimum 6 wejść i 6 wyjść przekaźnikowych.
- Oferowany system integrujący musi posiadać ważny:
- Krajowy Certyfikat Stałości Właściwości Użytkowych objęty Krajową Oceną Techniczną
- Świadectwo Dopuszczenia CNBOP

Oferowany system integrujący musi być możliwy do wdrożenia zgodnie z wytycznymi CNBOP „CNBOP–PIB W-0007:2020 Integracja Systemów Bezpieczeństwa Pożarowego Obiektów Budowlanych”.

Rozwiązanie musi umożliwiać współdziałanie wszystkich systemów w zakresie wizualizacji i sterowania, których działanie lub dezaktywacja jest wymagane w przypadku zagrożenia pożarowego i ma wpływ na bezpieczeństwo pożarowe obiektu.

11.1 Wymagania podstawowe aplikacji PSIM

1. Aplikacja PSIM musi współpracować z centralami sterującymi urządzeniami przeciwpożarowymi w sposób zgodny z punktem 12.1 załącznika do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 20 czerwca 2007 roku w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania.

2. Aplikacja PSIM musi być neutralna względem integrowanych systemów.

3. Aplikacja PSIM musi być otwarta, tzn. poza wspieraniem funkcji integracji systemów poprzez interfejsy natywne, aplikacja PSIM musi wspierać protokoły otwarte,

w tym: OPC, BACnet, KNX, Modbus RTU, Modbus IP, LON Bus.

4. Aplikacja PSIM musi być obsługiwana przez dedykowaną aplikację kliencką, wykonaną w technologii okienkowej.

Niedopuszczalne jest zastosowanie przeglądarki internetowej i technologii okien pop-up, celem eliminacji możliwości przechwycenia danych.

5. Aplikacja PSIM musi zapewniać możliwość całkowitego ukrycia systemu operacyjnego Windows przed operatorem.

6. Aplikacja PSIM musi zapewniać możliwość zdefiniowania hierarchii lokalizacji, celem uporządkowanego administrowania punktami danych oraz grupami czujników.

7. Aplikacja PSIM musi zapewniać przegląd punktów danych w dynamicznej strukturze drzewiastej, np. lokalizacja, typ systemu, grupa, czujnik.

8. Aplikacja PSIM powinna zapewniać możliwość pracy tle., co oznacza iż na stacji roboczej można opcjonalnie używać innych aplikacji, a w momencie wystąpienia zdarzenia/alarmu, głównie okno aplikacji PSIM przesunie się na wierzch, z alarm zostanie zasygnalizowany dodatkowo akustycznie i optycznie.

9. Aplikacja PSIM musi zapewniać szyfrowanie komunikacji co najmniej na poziomie bezpieczeństwa, jaki zapewnia algorytm AES256.

10. Aplikacja PSIM musi zapewniać możliwość outsourcingu uwierzytelniania użytkowników i administrowania ze pośrednictwem LDAP do Active Directory i zastosowanie profili użytkowników Active Directory.

11. Aplikacja PSIM powinien zapobiegać przedostawaniu się danych i poleceń do systemu z zewnątrz bez uzasadnienia, a także uniemożliwiać osobom trzecim dostęp do systemu. W ten sposób połączenia IP między serwerami i klientami będą szyfrowane przez TLS.
12. Aplikacja PSIM musi być dostępna w polskiej wersji językowej.
13. Aplikacja PSIM musi zapewniać możliwość obsługi zdarzeń za pomocą aplikacji mobilnej Android i iOS, z możliwością przesyłania zdjęć i automatycznego generowania zleceń.
14. Aplikacja PSIM musi oferować funkcjonalność monitorowania i wykorzystania pojemności środowiska sprzętowego aplikacji PSIM (CPU, RAM, HDD, LAN) przez sam system. W przypadku przekroczenia limitów wartości, system ma monitorować operatora o występującym problemie.
15. Aplikacja PSIM musi zapewniać pomoc kontekstową online.
16. Producent, a szczególnie proces projektowania i produkcji oprogramowania, powinien być objęty procedurą ISO 9001:2015. Do oferty należy załączyć aktualny certyfikat.
17. Należy załączyć oświadczenie Producenta oprogramowania PSIM, iż aplikacja spełnia wymagania europejskiej normy DIN EN 50518 dotyczącej PSIM, w zakresie ARC (Alarm Receiving Center, w polskiej nomenklaturze Centrum Monitorowania Alarmów (CMA)).

11.2 Cechy funkcjonalno-sprzętowe

- Integrator musi być wyposażony w zintegrowany moduł wentylacji aktywnej sterowany za pomocą termostatu.
- Integrator musi zapewniać wyświetlenie w aplikacji PSIM informacji o pracy na zasilaniu awaryjnym oraz sygnalizować otwarcie obudowy (kontrola nad potencjalnie nieautoryzowanym dostępem osób trzecich).
- Integrator musi umożliwiać komunikację Ethernet bez konieczności stosowania zewnętrznych konwerterów mediów.
- Integrator musi posiadać zabezpieczenia przeciwprzepięciowe chroniące transmisję szeregową RS485/RS232 realizowaną za pomocą portów COM.
- Integrator musi umożliwiać bezpośrednie podłączenie do 8 urządzeń/central komunikujących się z wykorzystaniem transmisji Ethernet za pomocą interfejsów typu 1000Base-T.
- Współpracując z aplikacją PSIM, integrator musi umożliwić operatorowi aktywację alarmu pożarowego drugiego stopnia (funkcja tzw. wirtualnego ROP-a)*. *funkcja zależy od zakresu funkcjonalnego interfejsów komunikacyjnych integrowanych systemów sygnalizacji pożaru
- Integrator musi umożliwiać użycie interfejsów HDMI oraz DVI do bezpośredniego podłączenia dwóch monitorów jednocześnie.

11.3 Prawa dostępu

1. Aplikacja PSIM musi pozwalać na definiowanie nieograniczonej liczby użytkowników, chronionych hasłem dostępu.
2. Użytkownik aplikacji PSIM, powinien mieć możliwość zmiany hasła po pierwszym logowaniu do systemu.
3. Aplikacja PSIM musi zapewniać możliwość zdefiniowania nieograniczonej

liczby profili użytkowników. Profil określa wygląd i funkcje dostępne z poziomu interfejsu systemu oraz definiuje wszystkie prawa użytkownika.

4. Aplikacja PSIM musi umożliwiać przypisanie kilku profili jednemu użytkownikowi, między którymi może się on przełączać w dowolnym momencie.

5. Aplikacja PSIM musi zapewniać możliwość ograniczenia bądź wskazania możliwości wyboru profili, na który operator może się zalogować.

6. Prawa dostępu i edycji oraz reguły powinny być przypisane do poszczególnych profili, a następnie propagowane na użytkowników.

11.4 Zarządzania zdarzeniami

1. Aplikacja PSIM musi posiadać centralny stos alarmów, z możliwością jego dostosowywania do potrzeb użytkownika (grupowanie i sortowanie zdarzeń).

2. Aplikacja PSIM musi zapewniać możliwość konfigurowania stosu alarmu, przy czym funkcjonalność ta powinna być ograniczona prawami dostępu.

3. Aplikacja PSIM musi zapewniać akustyczną i optyczną sygnalizację przychodzących zdarzeń.

4. Aplikacja PSIM musi zapewniać filtrowanie i grupowanie zdarzeń w ramach konfigurowalnych filtrów, w ramach stosu alarmowego, jak i samodzielnej formatki systemowej.

5. Aplikacja PSIM musi zapewniać wyświetlenie, w zależności od typu zdarzenia, określony typ grafiki (schemat, podgląd z kamery, mapa GIS, itp.), procedurę postępowania oraz informacje powiązane, w układzie przypisanym do danego użytkownika.

6. Aplikacja PSIM musi zapewniać możliwość dodania do danego zdarzenia dokumentów powiązanych (np. pdf, jpg, docs, xlsx) poprzez funkcję drag & drop, oraz bezpośrednich komentarzy dodawanych w ramach realizacji prac przez operatorów.

7. Aplikacja PSIM musi zapewnić możliwość szybkiego wydruku – przycisk funkcyjny na oknie zdarzenia, raportu ze zdarzenia, w dowolnym momencie jego realizacji, w postaci pliku PDF, zawierającego co najmniej: unikalny numer, log wszystkich zdarzeń (działania użytkownika), grafikami zdarzenia, zrzutami ekranowymi, komentarzami, zdjęciami oraz szczegółami wiadomości.

8. Aplikacja PSIM musi zapewniać możliwość definiowania przepływów pracy (workflow) bez żadnych ograniczeń w logikę, którą można zaprogramować (skomplikowanie procedur, liczba zmiennych, złożoność procesów).

9. Aplikacja PSIM musi zapewniać możliwość informowania o wystąpieniu określonego typu zdarzenia za pomocą sms'a oraz mail'em.

10. Aplikacja PSIM musi umożliwiać przejmowanie do realizacji zdarzeń przez danego pracownika (zdjęcie ze ogólnego stosu), przypisywanie zdarzeń (ręczne, jak i automatyczne).

11. Aplikacja PSIM musi zapewniać możliwość definiowania przedziałów czasowych koniecznych na realizację poszczególnych etapów zdarzenia oraz automatyczne informowanie w przypadku braku podjęcia działań przez operatora.

12. Aplikacja PSIM, poprzez aplikację mobilną, musi zapewniać wyzwalanie nowych zdarzeń oraz śledzenie istniejących z pełną dostępnością do np. powiązanych zdjęć, nagrań głosowych, filmów.

11.5 Operacje kontrolne

1. Aplikacja PSIM musi posiadać funkcjonalność planowania i automatyzacji

operacji kontrolnych i serwisowych, rozumianą jako możliwość jednorazowego lub cyklicznego wprowadzenia określonego typu punktu danych (np. kamera, czytnik kontroli dostępu) w określony stan. W ramach definiowania harmonogramu, uprawniony operator, musi mieć możliwość zdefiniowania czy ów działanie podlega każdorazowej akceptacji oraz czy rozpoczęcie, jak i zakończenie podlega każdorazowemu potwierdzeniu.

11.6 Grafika

- Aplikacja PSIM musi posiadać zintegrowany graficzny interfejs użytkownika (GUI).
- Aplikacja PSIM musi zapewniać modułową strukturę graficzną, tj, każda grafika może zostać wstawiona jako moduł do innej grafiki.
- Aplikacja PSIM musi zapewniać możliwość wyświetlania wielu treści jednocześnie tj. map, grafik, przycisków, paska narzędziowego, strony internetowej, kanałów RSS, stosu zdarzeń i alarmów, etc.
- GUI aplikacji PSIM musi zapewniać możliwość interakcji ze ścianami wizyjnymi w wykorzystaniem metody drag & drop.
- GUI aplikacji PSIM nie może ograniczać liczby wyświetlanych jednocześnie okien.
- GUI aplikacji PSIM nie może ograniczać liczby definiowanych widoków.
- Aplikacja PSIM musi zapewniać możliwość bezpośredniego osadzania grafiki, w standardowych formatach (.wmf, .emf, .sld, .bmp, .jpg, .png, .tif, .gif,) oraz formatach CAD (AutoCAD .dxf i .dwg oraz Microstation .dgn), w grafice aplikacji PSIM.
- Aplikacja PSIM musi zapewniać automatyczną aktywację symboli czujników i zmiany w grafikach wprowadzanych w połączonych z aplikacją plikami w formacie CAD.
- Aplikacja PSIM, poprzez edytor graficzny musi umożliwiać tworzenie własnych symboli oraz edytowanie już istniejących.
- Aplikacja PSIM powinna zapewniać podstawową bibliotekę symboli do różnych przypadków użycia.
- Aplikacja PSIM musi zapewniać możliwość wstawiania do grafik oraz tekstu przycisków z przypisanymi akcjami.
- Aplikacja PSIM musi zapewniać możliwość definiowania warstw, czyli pozwalając na logiczne grupowanie określonych typów informacji (np. typów punktów danych) i ich wyświetlanie bądź ukrywanie w zależności od przypadku użycia.

11.7 Archiwizacja

1. Aplikacja PSIM musi zapewniać pełną archiwizację przetwarzanych zdarzeń.
2. Aplikacja PSIM musi zapewniać możliwość filtrowania archiwum za pomocą zmiennych filtrów.
3. Aplikacja PSIM musi zapewniać wyświetlenie zarchiwizowanego zdarzenia ze wszystkimi powiązаныmi informacjami (takimi samymi jak podczas przetwarzania zdarzenia).
4. Aplikacja PSIM musi zapewniać logowanie wszystkich działań podejmowanych przez operatora.
5. Aplikacja PSIM musi zapewniać możliwość dostępu do poszczególnych lokalizacji, jak i punktów danych.

12 Instalacja telefoniczna

W pom. 1.12 na 1 piętrze w szafie GPD zabudować centralę telefoniczną.

Zabudowany moduł centrali powinien spełniać minimalne wymagania ogólne:

- Montaż centrali w szafie rack w serwerowni,
- System zdublowanej jednostki sterującej,
- minimum 100 abonenckich portów analogowych,
- 1 karta 4x E1,
- 1 licencja DSS1 (do połączeń z Multimedia)
- 1 licencja Q.sig,
- minimum 8 abonenckich portów systemowych Up0,
- Zespół wentylatorów,
- Zasilanie modułu zsieciovanego z podtrzymaniem bateryjnym na 4 godziny.

System w ramach sekcji wyniesionej musi zapewniać automatyczne zestawianie połączeń wewnętrznych, połączeń w ruchu wychodzącym i przychodzącym.

Wymagana jest minimum realizacja usług typu:

- bezpośrednie wybieranie numeru wewnętrznego (DDI),
- przekazywanie połączeń (CT) wraz z funkcją biura zleceń (przekazywanie połączeń zestawionych przez operatora),
- przenoszenie wywołań na numer wewnętrzny i zewnętrzny w przypadku zajętości (CFB), braku odpowiedzi (CFNR), bezwarunkowe (CFU), w tym przenoszenie wywołań na pocztę głosową,
- zawieszanie połączeń (CH),
- połączenie oczekujące (CW),
- prezentacja numeru na aparatach cyfrowych, voip i analogowych (FSK),
- przechwytywanie połączeń,
- połączenia trójstronne (3PTY),
- blokada połączeń przychodzących (DND),
- połączenia automatyczne typu gorąca linia (HOT LINE) realizowane bezzwłocznie, natychmiast po podniesieniu mikrotelefonu bez konieczności wybierania numeru lub ze zwłoką umożliwiającą wybranie numeru zaraz po podniesieniu mikrotelefonu.
- oddzwanianie przy zajętości (usługa CCBS) oraz przy braku odpowiedzi (usługa CCNR) – w przypadku zajętości (braku odpowiedzi) wywoływanego terminala w obrębie systemu abonent może na tle sygnału zajętości (CCBS) oraz na tle zwrotnego sygnału dzwonienia (CCNR) zażądać automatyczne zrealizowanie połączenia przez Serwer Telekomunikacyjny w chwili gdy terminal wywoływany przejdzie w stan spoczynku (CCBS) lub pojawi się jakakolwiek aktywność ze strony wywoływanego terminala (CCNR)
- Zestawianie połączeń telekonferencyjnych (dla min. 80 jednoczesnych uczestników):
 - automatyczne z listy (programowanie stałych grup telekonferencyjnych) oraz ręczne dobieranie uczestników konferencji wraz z:

- możliwością wizualizacji optycznej abonentów dołączonych u prowadzącego,
 - możliwością sterowania mikrofonem uczestnika konferencji przez prowadzącego (np. domyślnie wszyscy uczestnicy jedynie słuchają),
 - możliwością wysłania do prowadzącego żądania prawa głosu przez uczestnika konferencji,
- dynamiczne – organizacja konferencji wdzwanianej typu „meet-me” z podaniem hasła, konferencja jest zamawiana przez dowolnego użytkownika systemu na określonym numerze dostępowym wraz z definiowaniem hasła, możliwość wdzwonienia się do konferencji z zewnątrz (z sieci PSTN/GSM).
- Wirtualne logowanie - realizacja połączeń z dowolnego aparatu z wykorzystaniem posiadanych uprawnień (przypisanie opłat taryfikacyjnych na rachunek dokonującego połączenie) – autoryzacja odbywa się poprzez wprowadzenie kodów PIN. Usługa musi umożliwiać zalogowanie się jednokrotne (na czas wykonania 1 połączenia) lub permanentne do czasu wylogowania się.
- Programowe wydzielanie grup abonentów o dowolnej liczebności – na zasadzie podziału firmy na wydziały/jednostki z możliwością wydzielenia zasobów, przypisania odrębnego planu numeracyjnego, kategorii uprawnień i nawet zabronienia dzwonienia po numerach wewnętrznych pomiędzy nimi.
- Możliwość kolejkowania połączeń przychodzących dla wydzielonej grupy abonentów.
- Tworzenie grup abonentów (min. 10 grup po 30 użytkowników w dowolnej kombinacji abonentów) z automatyczną dystrybucją połączeń w ramach grupy zgodnie z różnymi algorytmami.
- Przechwytywanie połączeń w ramach grupy – w przypadku wywołania na jednym z terminali abonenckich, musi być możliwe przejęcie tego wywołania przez dowolny inny terminal z tej samej grupy.
- Możliwość zdefiniowania minimum 10 różnych kategorii określających uprawnienia realizacji połączeń wyjściowych nadawanych poszczególnym użytkownikom w systemie (np. blokada połączeń wychodzących, blokada połączeń na komórki, blokada połączeń międzynarodowych itd.)
- Tworzenie układów połączeń sekretarsko–dyrektorskich oraz układów dyspozytorskich
- Monitorowanie stanu linii abonenckich lub łączy za pomocą aparatów wyposażonych w klawisze programowalne z sygnalizacją optyczną lub przystawki z klawiszami programowalnymi z sygnalizacją optyczną.
- Konfiguracja systemu musi odbywać się z poziomu dedykowanej, graficznej aplikacji pracującej pod systemami MS Windows 7/8/10/11. Ze względów bezpieczeństwa niedopuszczalne jest używanie do konfiguracji systemu rozwiązań wykorzystujących przeglądarki www. Aplikacja musi posiadać interfejs graficzny w języku polskim.
- System musi być wyposażony w centralną książkę telefoniczną opartą na protokole LDAP.
- Możliwość rozbudowy o:

- Aplikację CTI użytkownika
- Poczta głosową
- Faks serwer
- System rejestracji rozmów

Centralna książka telefoniczna będzie modulem SUD i będzie działać w oparciu o standardowy protokół LDAP. Centralna książka telefoniczna jest instalowana i uruchamiana w całym systemie (centrale i sekcje (moduły) wyniesione).

CKT umożliwia podział na:

- część globalną – dostępną dla każdego użytkownika,
- część grupową – dostępną dla określonej grupy użytkowników,
- część prywatną – dostępną jedynie dla konkretnego użytkownika.

Dostęp do centralnej książki telefonicznej jest możliwy z:

- cyfrowych telefonów systemowych,
- klientów poczty elektronicznej Outlook, Thunderbird,
- strony WWW,
- aparatów IP z wyświetlaczem,
- aplikacji CTI Asystent DGT,
- konsol dyspozytorskich,
- Możliwość przypisywania do określonych kontaktów w CKT zdjęcia (plik graficzny) i opisów słownych.
- CKT umożliwia integrację z kontrolerami domeny ActiveDirectory.

13 Okablowanie instalacji niskoprądowych

Całość okablowania wszystkich instalacji niskoprądowych przebiegającego w drogach ewakuacyjnych jak i poza nimi wykonać w klasie CPR B2 ca s1 d1 a1.

Ponadto dla przewodów nie objętych normą PN-EN 50575 (przewody FE180, E20/60/90, PH90) oraz certyfikowanych zespołów kablowych obejmujących kable wraz ze sposobem ich montażu stosowanie ich będzie odbywać się na podstawie Krajowych Deklaracji Własności Użytkowych i Świadectw Dopuszczenia.

14 Wymagania środowiskowe

14.1 Ogólne założenia

Planowana realizacja przedsięwzięcia inwestycyjnego musi być zgodna z zasadą „nie czyni poważnej szkody” w rozumieniu art. 17 rozporządzenia (UE) nr 2020/852 (rozporządzenie w sprawie taksonomii) [ang. „Do No Significant Harm” (DNSH)], w tym:

1. Realizacja przedsięwzięcia nie może prowadzić do znaczących emisji gazów cieplarnianych. (Cel: Łagodzenie zmian klimatu)
2. Realizacja przedsięwzięcia nie może prowadzić do nasilenia niekorzystnych skutków obecnych i oczekiwanych, przyszłych warunków klimatycznych, wywieranych na tę działalność lub na ludzi, przyrodę lub aktywa. (Cel: Adaptacja do zmian klimatu)
3. Realizacja przedsięwzięcia nie może szkodzić:
 - a) dobremu stanowi lub dobremu potencjałowi ekologicznemu jednolitych części wód, w tym wód powierzchniowych i wód podziemnych,

- b) dobremu stanowi środowiska wód morskich. (Cel: Zrównoważone wykorzystanie i ochrona zasobów wodnych i morskich)
- 4. Realizacja przedsięwzięcia nie może prowadzić do:
 - a) znaczącego braku efektywności w wykorzystywaniu materiałów lub w bezpośrednim lub pośrednim wykorzystywaniu zasobów naturalnych, takich jak nieodnawialne źródła energii, surowce, woda i grunty, na co najmniej jednym z etapów cyklu życia produktów, w tym pod względem trwałości produktów, a także możliwości ich naprawy, ulepszenia, ponownego użycia lub recyklingu,
 - b) znacznego zwiększenia wytwarzania, spalania lub unieszkodliwiania odpadów, z wyjątkiem spalania odpadów niebezpiecznych nienadających się do recyklingu,
 - c) długotrwałego składowania odpadów mogących wyrządzać poważne i długoterminowe szkody dla środowiska. (Cel: Gospodarka o obiegu zamkniętym, w tym zapobieganie powstawaniu odpadów i recykling)
- 5. Realizacja przedsięwzięcia nie może prowadzić do znaczącego wzrostu emisji zanieczyszczeń do powietrza, wody lub ziemi w porównaniu z sytuacją sprzed rozpoczęcia przedsięwzięcia. (Cel: Zapobieganie zanieczyszczeniom powietrza, wody lub gleby i jego kontrola)
- 6. Realizacja przedsięwzięcia:
 - a) nie może szkodzić (w znacznym stopniu) dobremu stanowi i odporności ekosystemów,
 - b) nie może być szkodliwa dla stanu zachowania siedlisk i gatunków, w tym siedlisk i gatunków objętych zakresem zainteresowania Unii Europejskiej. (Cel: Ochrona i odbudowa bioróżnorodności i ekosystemów)
- 7. Do realizacji celu środowiskowego w postaci łagodzenia zmian klimatu, wyrażonego w art. 9 lit. a Rozporządzenia DNSH, Wykonawcę zobowiązuje się w szczególności do zapewnienia efektywności energetycznej poprzez zastosowanie energooszczędnych urządzeń i systemów m.in. oświetlenia LED i inteligentnych systemów zarządzania energią oraz do zapewnienia wykorzystania odnawialnych źródeł energii poprzez instalacje paneli fotowoltaicznych.
- 8. Do realizacji celu środowiskowego w postaci adaptacji do zmian klimatu, wyrażonego w art. 9 lit. b Rozporządzenia DNSH, Wykonawcę zobowiązuje się w szczególności do zapewnienia odporności systemów i wykonania instalacji z myślą o odporności na ekstremalne zjawiska pogodowe, jak burze, czy powodzie oraz do redundacji poprzez wprowadzenie systemów zapasowych, które zapewnią ciągłość działania w razie awarii głównej instalacji takich jak UPS-y, czy agregaty prądotwórcze.
- 9. Do realizacji celu środowiskowego w postaci przejścia na gospodarkę o obiegu zamkniętym, wyrażonego w art. 9 lit. d Rozporządzenia DNSH, Wykonawcę zobowiązuje się w szczególności do recyklingu i ponownego wykorzystania materiałów ku minimalizacji odpadów poprzez odpowiednie zarządzanie nimi i przekazywanie do recyklingu oraz do zastosowania trwałych materiałów o długim okresie użytkowania i niskim wpływie na środowisko. Co najmniej 70 % (masy) innych niż niebezpieczne odpadów z budowy i rozbiórki (wyluczając naturalnie występujące materiały, o których mowa w kategorii 17 05 04 w

europejskim wykazie odpadów ustanowionym w decyzji 2000/532/WE) wytwarzanych na placu budowy jest gotowe do ponownego użycia, recyklingu i innych procesów odzysku materiału, takich jak operacje wypełniania wykopów z wykorzystaniem odpadów zastępujących inne materiały, zgodnie z hierarchią postępowania z odpadami i Protokołem UE dotyczącym gospodarowania odpadami z budowy i rozbiórki (588). Operatorzy ograniczają wytwarzanie odpadów w procesach związanych z budową i rozbiórką, zgodnie z Protokołem UE dotyczącym gospodarowania odpadami z budowy i rozbiórki oraz uwzględniając najlepsze dostępne techniki i stosując selektywną rozbiórkę w celu umożliwienia usunięcia substancji niebezpiecznych i bezpiecznego postępowania z nimi oraz ułatwienia ponownego użycia i wysokiej jakości recyklingu w drodze selektywnego usuwania materiałów z wykorzystaniem dostępnych systemów sortowania odpadów z budowy i rozbiórki.

10. Do realizacji celu środowiskowego w postaci zapobiegania zanieczyszczeniom i ich kontroli, wyrażonego w art. 9 lit. e Rozporządzenia DNSH, Wykonawcę zobowiązuje się w szczególności do stosowania bezpiecznych substancji i unikania szkodliwych substancji chemicznych, takich jak PCB stosowane w starych instalacjach oraz kontroli emisji poprzez zastosowanie technologii zmniejszającej emisji szkodliwych substancji do atmosfery, w szczególności urządzeń zasilanych energią elektryczną. Elementy budynków i materiały budowlane wykorzystane przy budowie są zgodne z kryteriami określonymi w dodatku C do niniejszego załącznika do Rozporządzenia DNSH w tym: elementy budynków i materiały budowlane wykorzystane przy renowacji budynku, z którymi mieszkańcy mogą mieć kontakt (590), emitują mniej niż 0,06 mg formaldehydu na m³ materiału lub elementu na podstawie badania zgodnie z warunkami określonymi w załączniku XVII do rozporządzenia (WE) nr 1907/2006 oraz mniej niż 0,001 mg innych rakotwórczych lotnych związków organicznych kategorii 1A i 1B na m³ materiału lub elementu, co należy ustalić w ramach badań przeprowadzonych zgodnie z normą CEN/EN 16516 i ISO 16000-3:2011 (591) lub innymi równoważnymi znormalizowanymi warunkami badania i metodami oznaczania. Należy wprowadzić środki służące redukcji emisji hałasu, kurzu i zanieczyszczeń w trakcie robót budowlanych lub konserwacyjnych.
11. Do realizacji celu środowiskowego w postaci ochrony i odbudowy bioróżnorodności biologicznej oraz ekosystemów, wyrażonego w art. 9 lit. f Rozporządzenia DNSH, Wykonawcę zobowiązuje się w szczególności do zapewnienia minimalizacji wpływu na lokalne ekosystemy poprzez unikanie ingerencji w lokalne siedliska podczas modernizacji instalacji lub nowej budowy.

14.2 Obowiązki wykonawcy

Wykonawca zobowiązuje się do przedłożenia Zamawiającego deklaracji właściwości użytkowych, będących dokumentacją zawierającą potwierdzenie, że wyroby budowlane spełniają normy i posiadają wymagane właściwości, zwłaszcza dla substancji niebezpiecznych, wydawane w oparciu o przepisy ustawy z dnia 16 kwietnia 2004 r. o wyrobach budowlanych (t.j. Dz. U. z 2021 r.

poz. 1213) oraz wyników badań gruntów lub informacji o wynikach badań ekofizjograficznych sporządzonych na potrzeby planu miejscowego obejmującego miejsce budowy, jak również dokumentacji wydanej przez urząd miasta, poświadczającej, że grunt, na którym odbywać się ma budowa, spełnia wymagania z zakresu ochrony bioróżnorodności.

Wykonawca zobowiązany jest do sporządzenia wykazu działań skutecznie zapobiegających emisji hałasu, kurzu i zanieczyszczeń występujących wskutek realizacji zaplanowanych robót budowlanych i mających wpływać na efektywne obniżenie natężenia czynników negatywnych i prowadzić do ich całkowitego wyeliminowania, dzięki wykorzystaniu najlepszych dostępnych technik, będących dokumentacją dotyczącą gospodarki odpadami, zawierająca listę rozwiązań, jakie będą stosowane podczas wykonywania robót w celu obniżenia natężenia czynników negatywnych bądź prowadzić do całkowitego ich wyeliminowania, w szczególności:

- 1) zabezpieczenie surowców sypkich składowanych na placu budowy przed wiatrem,
- 2) osłonięcie miejsc prowadzenia robót, w których następuje emisja pyłów,
- 3) prowadzenie robót z pominięciem godzin nocnych,
- 4) kontrolowanie poziomu emitowanego hałasu, zabezpieczenie miejsc, gdzie przechowywane są paliwa,
- 5) uniemożliwienie przenikania paliw i innych substancji do gruntu i wód przypowierzchniowych,
- 6) kontrolowanie odprowadzania zanieczyszczonych wód z terenu budowy.

14.3 Opracowania, do których sporządzenia zobowiązuje się Wykonawcę

1. Analizę dotyczącą wpisywania się w gospodarkę o obiegu zamkniętym, będącą analizą opartą o model produkcji i konsumpcji, polegającą na ponownym użyciu, naprawie, odnawianiu i recyklingu istniejących materiałów i produktów tak długo, jak to możliwe, celem wydłużenia się cyklu życia materiałów budowlanych;
2. Analizę ryzyka wynikającego ze zmian klimatu, będącą analizą zawierającą:
 - a) ryzyka klimatyczne, jakie mogą wystąpić w miejscu, w którym zlokalizowany jest przedmiot inwestycji w okresie, w jakim budynek będzie użytkowany,
 - b) ocenę zagrożeń klimatycznych, jakie mogą wpłynąć na realizowaną inwestycję oraz wpływ na nią w czasie jej użytkowania takich czynników jak: wysokie temperatury w miesiącach letnich, zwiększona liczba upalnych dni w roku, silne wiatry, zaleganie pokrywy śnieżnej, powodzie,
 - c) plan adaptacji, będący wyszczególnieniem rozwiązań, jakie zostały zastosowane w budynku, albo które będą realizowane w przyszłości, aby minimalizować ryzyko mogących się pojawić niekorzystnych oddziaływań klimatycznych;
3. Analizę rozwiązań technicznych planowanych robót w oparciu o normę: „ISO 20887:2020, Zrównoważony charakter budynków i robót budowlanych związanych z inżynierią lądową – Projektowanie do celów możliwości demontażu i adaptacji – Zasady, wymagania i wytyczne” oraz gromadzoną i aktualizowaną w całym cyklu życia budynków będących

przedmiotem robót, dokumentację zawierającą:

- a) opis rozwiązań i instrukcje, które na etapie rozbiórki budynku umożliwiać będą prowadzenie prac w taki sposób, który pozwoli na odzyskanie możliwie jak największej części materiałów, segregację, ponowne wykorzystanie lub recykling,
 - b) listę rodzajów materiałów i ich ilości, które zostaną wbudowane, co ma pozwolić na ich identyfikowalność na etapie prowadzenia napraw, kolejnych remontów i rozbiórki,
 - c) opis potencjału budynku do adaptacji do nowych funkcji w cyklu życia;
4. Audytu przedrozbiórkowego, będącego analizą obiektów przed planowaną rozbiórką, sporządzana w odniesieniu do robót budowlanych poprzedzonych rozbiórką części budynków lub jego elementów, służąca identyfikacji odpadów, jakie mogą się pojawić i ich ilości, wskazaniu wyrobów, które mogą zostać ponownie użyte oraz zawierająca zasady i sposoby segregacji surowców pozyskanych z rozbiórki, jak również możliwości zagospodarowania odpadów zgodnie z hierarchią postępowania z odpadami (jeżeli zajdzie potrzeba robót rozbiórkowych);
 5. Świadectwa charakterystyki energetycznej, będącego dokumentem określającym wielkość zapotrzebowania na energię niezbędną do zaspokojenia potrzeb energetycznych związanych z użytkowaniem budynku lub części budynku, wskazująca na zapotrzebowanie po przeprowadzeniu robót budowlanych, sporządzana przez osobę wpisaną do rejestru osób uprawnionych do sporządzania świadectw charakterystyki energetycznej budynków a sporządzony w oparciu o przepisy ustawy z dnia 29 sierpnia 2014 r. o charakterystyce energetycznej budynków (t.j. Dz. U. z 2024 r. poz. 101);
 6. Zestawienia materiałów i przedmiaru, będącego dokumentacją zawierającą kompletne zestawienie wszystkich prac budowlanych niezbędnych do realizacji inwestycji, przedstawionych w kolejności technologicznej wykonywania prac, obejmujący m.in. ceny materiałów oraz ceny robocizny, wraz z podstawą do naliczenia poszczególnych opłat;
 7. Wykazu odpadów i planu segregacji odpadów w oparciu o zestawienie materiałów i przedmiaru, będącego dokumentacją dotyczącą gospodarki odpadami, zawierająca listę rozwiązań, jakie będą stosowane podczas wykonywania robót w celu obniżenia natężenia czynników negatywnych bądź prowadzić do całkowitego ich wyeliminowania, w szczególności:
 - a) zabezpieczenie surowców sypkich składowanych na placu budowy przed wiatrem,
 - b) osłonięcie miejsc prowadzenia robót, w których następuje emisja pyłów,
 - c) prowadzenie robót z pominięciem godzin nocnych,
 - d) kontrolowanie poziomu emitowanego hałasu, zabezpieczenie miejsc, gdzie przechowywane są paliwa,
 - e) uniemożliwienie przenikania paliw i innych substancji do gruntu i wód przypowierzchniowych,
 - f) kontrolowanie odprowadzania zanieczyszczonych wód z terenu budowy;
 8. Opracowania wskazującego na przeprowadzenie oceny śladu

węglowego budynku w pełnym cyklu życia, będącego dokumentacją określającą wyliczenia w zakresie śladu węglowe nowo wybudowanych budynków w pełnym cyklu życia, sporządzona zgodnie z normą EN 15978 „Zrównoważone obiekty budowlane – Ocena środowiskowych właściwości użytkowych budynków – Metoda obliczania”.

Współczynnik globalnego ocieplenia przedstawia się w postaci liczbowego wskaźnika w odniesieniu do każdego etapu cyklu życia wyrażonego w kg ekwiwalentu dwutlenku węgla/m² (wewnętrznej powierzchni użytkowej), uśrednionego dla jednego roku w referencyjnym okresie badania wynoszącym 50 lat. Dobór danych, określenie scenariuszy i obliczenia przebiegają zgodnie z normą EN 15978 (BS EN 15978:2011 Zrównoważone obiekty budowlane – Ocena środowiskowych właściwości użytkowych budynków – Metoda obliczania).

Ocena potencjału globalnego ocieplenia (GWP) powinna zostać wykonana indywidualnie dla każdego etapu cyklu życia, z rozróżnieniem na emisję gazów cieplarnianych pochodzenia biogenicznego oraz wynikających z wykorzystania surowców kopalnych, użytkowania i przekształcania gruntów.

Granice systemu powinny uwzględniać zakres zdefiniowany dla poziomu 2 lub 3 europejskiego systemu oceny budynków Level(s), zaś prezentowane wyniki powinny być opatrzone informacją na temat zakresu oddziaływań.

Deklaracje Środowiskowe III Typu, opracowane zgodnie z wytycznymi ISO 14025 Etykiety i deklaracje środowiskowe -- Deklaracje środowiskowe III typu -- Zasady i procedury mogą być stosowane jako dane wejściowe do oceny.

Ocena śladu węglowego budynku może być wykonana za pomocą zwalidowanej metody obliczeniowej lub komercyjnie dostępnego oprogramowania, spełniającego minimalne wymagania schematu oceny Level(s).

Prezentowane wyniki GWP powinny dotyczyć najbardziej obciążającej konfiguracji systemu, przy czym mogą być uzupełnione o wyniki opisujące docelową konfigurację systemu, która co do zasady powinna prowadzić do zmniejszenia oddziaływań środowiskowych.

9. Wyniki badań gruntów lub informacja o wynikach badań ekofizjograficznych sporządzonych na potrzeby planu miejscowego obejmującego docelową działkę
10. Dokument wydawany przez urząd miasta, poświadczający, że grunt spełnia wymagania z zakresu ochrony bioróżnorodności
11. Wykaz działań skutecznie zapobiegających emisji hałasu, kurzu i zanieczyszczeń
12. Deklaracje właściwości użytkowych lub krajowe deklaracje właściwości użytkowych lub inne dokumenty potwierdzające posiadanie wymaganych właściwości przez wyroby budowlane (dla wyrobów związanych z wodą lub zawierających substancje niebezpieczne)
13. Analiza dotycząca wpisywania się w gospodarkę o obiegu zamkniętym (możliwości w zakresie demontażu obiektu lub dostosowania budynków zgodnie z ISO 20887)
14. Powykonawczy obmiar robót z podziałem na rodzaje wyrobów, ich ilości i masę
15. Jakościowe i ilościowe zestawienie materiałowe

15 Uwagi końcowe

- Całość prac wykonać zgodnie z obowiązującymi przepisami i normami.
- Przed rozpoczęciem robót wykonawca zobowiązany jest do zapoznania się z treścią uzgodnień z gestorami urządzeń podziemnych i bezwzględnego przestrzegania zawartych w nich uwag i warunków prowadzenia robót.
- Wszystkie materiały i urządzenia użyte do realizacji zamówienia muszą posiadać świadectwa dopuszczenia do obrotu i stosowania w budownictwie na obszarze rynku Polski/UE;
- Zastosowane materiały muszą posiadać odpowiednie: deklaracje zgodności, atesty, aprobaty techniczne, certyfikaty; materiały muszą spełniać parametry techniczne dopuszczające je do stosowania w budownictwie na obszarze rynku Polski/UE;
- Przed oddaniem do eksploatacji wykonać niezbędne pomiary tj. rezystancji izolacji przewodów, ciągłości żył, skuteczności ochrony przeciwporażeniowej, rezystancji obwodów, rezystancji uziemień itp. wystawiając odpowiednie protokoły pomiarów.
- W trakcie prac zwrócić uwagę na właściwą koordynację robót zwłaszcza z branżą c.o. wentylacji oraz wod. kan.
- Przy wykonywaniu przebić przez ściany oraz przy podwieszaniu korytek zwrócić uwagę, aby prowadzone prace nie naruszyły części konstrukcyjnej budynku.
- Wszystkie przejścia przewodów i kabli przez przegrody ogniowe muszą być uszczelnione specjalnymi masami ogniochronnymi o odporności ogniowej równej odporności przegrody, przez którą są prowadzone.

OPRACOWAŁ
inż. Marek Goncerzewicz