



ATELIER ARCHITEKTURY

ANNA JURCZYK - LECH
ul. T. Zawadzkiego 69/5
71-246 Szczecin
tel. 48 501 085 665

e-mail: annajurczykajl@wp.pl

PW-PROJEKT WYKONAWCZY-INSTALACJE NISKOPRĄDOWE

Tytuł projektu: Termomodernizacja i przebudowa budynku Katedry i Zakładu Anatomii Prawidłowej Klinicznej Pomorskiego Uniwersytetu Medycznego w Szczecinie.

Zadanie: SYSTEMY ZABEZPIECZEŃ TECHNICZNYCH SWiN, KD, CCTV

Inwestor: Pomorski Uniwersytet Medyczny w Szczecinie
ul. Rybacka 1, 70-204 Szczecin,

Adres inwestycji: al. Powstańców Wielkopolskich 72 w Szczecinie,

Kategoria obiektu budowlanego: IX

Zakres opracowania	Projektował	Podpis	<i>Sprawdził</i>	Podpis
Projekt wykonawczy INSTALACJE NISKOPRĄDOWE	mgr inż. Marek Chromiński Wpis na listę PZT-3878		tech. Piotr Pawłowski Wpis na listę PZT-6488	

OŚWIADCZENIE

Na podstawie art. 34 ust. 3d pkt. 3 Prawo Budowlane (Dz. U. 2023 poz. 682 tekst jednolity) – oświadczamy, że niniejszy projekt branży sanitarnej został opracowany zgodnie z obowiązującymi przepisami i zasadami wiedzy technicznej.

Data opracowania: grudzień 2023

Spis zawartości

A. CZĘŚĆ OPISOWA	4
1. PRZEDMIOT INWESTYCJI	4
1.1. Inwestor / Zamawiający	4
1.2. Podstawa opracowania	4
1.3. Uwarunkowania wstępne stanowiące podstawę opracowania	4
1.4. Zakres opracowania	5
1.5. Obowiązujące przepisy i normy branżowe	6
2. OGÓLNE ZAŁOŻENIA PROJEKTOWANYCH SYSTEMÓW	8
3. INSTALACJA MONITORINGU WIZYJNEGO CCTV	9
3.1. Koncepcja dozoru wizyjnego	9
3.2. Struktura instalacji	10
3.3. Dobór rozwiązań technicznych	11
3.4. Dobór urządzeń	13
3.4.1. Kamer stacjonarna zewnętrzna	13
3.4.2. Kamera stacjonarna wewnętrzna	13
3.4.3. Kamera dyskretna wewnętrzna	13
3.4.4. Rejestracja wizji	13
3.4.5. Prezentacja wizji	17
3.4.6. Ochronnik przeciwprzepięciowy	21
3.5. wytyczne montażowe	21
3.6. Zasilanie systemu monitoringu wizyjnego	21
3.7. Zestawienie materiałów - CCTV	22
4. INSTALACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM - SMS	23
4.1. Uwarunkowania wstępne projektowanego systemu	23
4.2. Projektowana realizacja uwzględniająca strategię Inwestora	25
5. INSTALACJA SYSTEMU KONTROLI DOSTĘPU – SKD	26
5.1. Koncepcja sterowania dostępem	26
5.2. Dobór zastosowanych rozwiązań – system SKD	26
5.2.1. czytnik zbliżeniowy,	26
5.2.2. kontroler KD,	27
5.2.3. sterownik sieciowy KD,	27
5.2.4. Przycisk wyjścia	28
5.2.5. Przycisk ewakuacyjny	28
5.2.6. Czujniki kontaktronowe	28
5.2.7. Elementy wykonawcze,	28
5.2.8. Elementy wykonawcze,	29

5.2.9.	Zasilacze buforowe,.....	29
5.2.10.	Oprogramowanie zarządzające systemem KD	29
5.2.11.	Karty bezstykowe autoryzacji dostępu	33
5.2.12.	Okablowanie	33
5.3.	Bilans energetyczny	34
5.4.	Struktura sieciowa instalacji KD	35
5.5.	Zestawienie materiałów - SKD	36
6.	INSTALACJA SYSEMU INTERKOMOWEGO.....	37
6.1.	Dobór zastosowanych rozwiązań – system interkomowy	37
6.1.1.	Panel przywoławczy systemu cyfrowego,.....	37
6.1.2.	Odbiornik interkomu,	38
6.1.3.	Filtr przeciwzakłóceńowy.	38
6.1.4.	zasilacz,.....	38
6.2.	Wytyczne montażowe	38
6.3.	Zestawienie materiałów - INTERKOMY	38
7.	INSTALACJA SYSTEMU SYGNALIZACJI WŁAMANIA SWiN	39
7.1.	Koncepcja systemu SWiN	39
7.2.	Wymagania dla projektowanego systemu SWiN	39
7.3.	Dobór zastosowanych rozwiązań – system SWiN	39
7.3.1.	Centrala alarmowa	39
7.3.2.	koncentrator i klaster central alarmowych.....	40
7.3.3.	Szyfrator OLED.....	41
7.3.4.	Expander wejść/wyjść z zasilaczem	42
7.3.5.	Czujniki kontaktronowe	42
7.3.6.	Detektory ruchu	42
7.3.7.	Detektory ruchu dualny	43
7.3.8.	Detektory uderowy (inercyjny)	43
7.3.9.	Czujnik zalania	43
7.3.10.	Sygnalizator optyczno-akustyczny	43
7.4.	Bilans energetyczny.....	43
7.5.	Wytyczne montażowe	44
7.6.	Zestawienie materiałów – SWiN.....	45
7.7.	Okablowanie instalacji niskoprądowych.....	45
B.	CZĘŚĆ GRAFICZNA	46

A. CZĘŚĆ OPISOWA

1. PRZEDMIOT INWESTYCJI

Przedmiotem inwestycji jest:

„Kompleksowa termomodernizacja i przebudowa budynku Katedry i Zakładu Anatomii Prawidłowej Klinicznej Pomorskiego Uniwersytetu Medycznego w Szczecinie”,

Inwestycja jest zlokalizowana w Szczecinie, przy al. Powstańców Wielkopolskich 72.

Projektowany budynek zakwalifikowano wg załącznika do ustawy z dnia 7 lipca 1994 r. Prawo budowlane jako obiekt kategorii IX - budynki kultury, nauki i oświaty.

1.1. Inwestor / Zamawiający

POMORSKI UNIWERSYTET MEDYCZNY w SZCZECINIE
ul. Rybacka 1, 70-204 Szczecin

1.2. Podstawa opracowania

- Umowa z Inwestorem
- Decyzja nr 49/22 z dnia 28.12.2022 r. o ustaleniu lokalizacji inwestycji celu publicznego
- Opis przedmiotu zamówienia- wytyczne technologiczne Inwestora
- Aktualne obowiązujące normy i wytyczne,
- Wizja lokalna w terenie, pomiary własne.
- Uzgodnienia międzybranżowe.
- Notatka służbowa nr 1 spisana z Inwestorem i Użytkownikiem 12. 12. 2022 r.
- Notatka służbowa nr 2 spisana z Inwestorem i Użytkownikiem w dniu 13.03.2023r.
- Projekty branżowe architektoniczne i instalacyjne,
- Wieloletnia koncepcja rozwoju systemów bezpieczeństwa PUM,
- Obowiązujące normy i przepisy

1.3. Uwarunkowania wstępne stanowiące podstawę opracowania

Systemy teletechniczne projektowane dla „Kompleksowa termomodernizacja i przebudowa budynku Katedry i Zakładu Anatomii Prawidłowej Klinicznej Pomorskiego Uniwersytetu Medycznego w Szczecinie”, stanowią kontynuacją wcześniej zaprojektowany 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, systemami Centrum Symulacji Medycznych oraz powstającego Budynku Kliniczno-Dydaktyczno-Badawczego PUM przy ul. Unii Lubelskiej. 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 oraz częściowo jeden obszar w budynku szpitala SPSK1, 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 prze-projektowania poniesie wykonawca wprowadzający zmiany.

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

1.4. Zakres opracowania

Zakresem niniejszego opracowania jest projekt wykonawczy instalacji zabezpieczeń technicznych, a w tym:

- monitoringu wizyjnego CCTV,
- kontroli dostępu obejmującej instalacje KD,
- sygnalizacji włamania i napadu SWiN

1.5. Obowiązujące przepisy i normy branżowe

Gdziekolwiek w specyfikacji technicznej oraz dokumentacji projektowej wskazane są konkretne normy i przepisy, które spełniać mają materiały, sprzęt i inne towary oraz wykonane i żądane roboty, będą obowiązywać postanowienia najnowszego wydania lub poprawionego wydania powołanych norm i przepisów. W przypadku gdy wskazane normy i przepisy są państwowe lub odnoszą się do konkretnego kraju lub regionu, mogą być również stosowane inne odpowiednie normy zapewniające równy lub wyższy poziom wykonania niż powołane normy lub przepisy, pod warunkiem ich sprawdzenia i pisemnego zatwierdzenia. Różnice pomiędzy wskazanymi normami a ich proponowanymi zamiennikami muszą być dokładnie opisane przez Wykonawcę, w szczególności poprzez dodanie słowa "lub równoważne", a następnie opisanie kryteriów stosowanych w celu oceny tej równoważności. Opis norm, przepisów i cech ich równoważności muszą zostać przedłożone do zatwierdzenia przez Zamawiającego.

Jeżeli w opracowaniach projektowych pojawiają się nazwy własne urządzeń lub stosowanych technologii, to zostały one wykorzystane wyłącznie do przeprowadzenia niezbędnych obliczeń i symulacji funkcjonalnych. Jednakże warunkiem wskazania w dokumentacji projektowej nazw własnych urządzeń lub stosowanych technologii jest dodanie słowa "lub równoważne" a następnie opisanie kryteriów stosowanych w celu oceny tej równoważności oraz wymogu ich zatwierdzenia przez Zamawiającego, jak w przypadku wskazania na konkretne normy i przepisy.

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

2. OGÓLNE ZAŁOŻENIA PROJEKTOWANYCH SYSTEMÓW

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

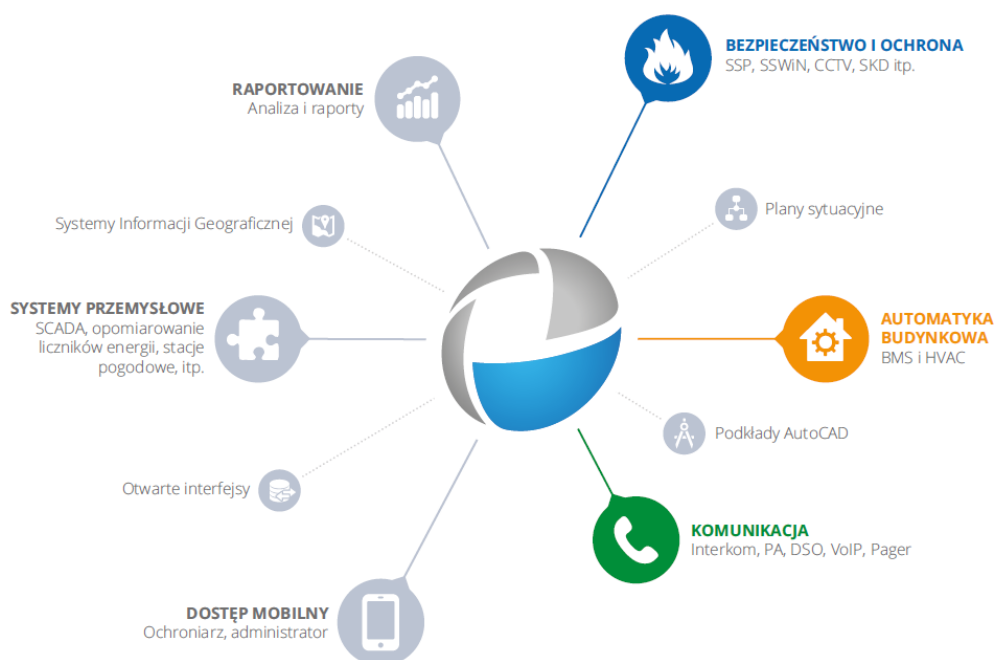
Charakter zrealizowanych budynków Centrum Symulacji Medycznych, budynku Międzywydziałowego Centrum Dydaktyki nr 3 oraz powstającego Budynku Kliniczno-Dydaktyczno-Badawczego przy ulicy Unii Lubelskiej wymusza jakościowe spojrzenie zarówno w obszarze inwestycji CapEx, ale także w kosztach utrzymania obiektu 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.

Jednak ze względu na założenie, iż w powstającym obecnie Budynku Kliniczno-Dydaktyczno-Badawczym przy ulicy Unii Lubelskiej docelowo ma się mieścić Centrum Zarządzania z wykorzystaniem rozwiązania klasy PSIM, już na obecnym etapie zaprojektowano instalację systemu PSIM umożliwiającego uruchomienie go zgodnie z koncepcją rozwoju systemów bezpieczeństwa.

Docelowo oprogramowanie PSIM miałyby obejmować swym zasięgiem następujące obszary, które integruje w ramach SMS



3. INSTALACJA MONITORINGU WIZYJNEGO CCTV

W przyjętej koncepcji zakłada się, iż projektowany system monitoringu wizyjnego będzie wykonywany 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 składa 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 obiektów dla podglądu dostępnych obrazów;

Platforma monitoringu stanowi 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 zapewnia obsługę min 30 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 wspiera obsługę protokołu ONVIF G, S, T. Dla bezpieczeństwa transmisji pomiędzy serwerem a kamerą możliwa jest transmisja z wykorzystaniem protokołu HTTPS.

Ponadto wykorzystywane są wbudowanych w kamerę algorytmy badania i jakości obrazu kamery w celu ułatwienia zarządzania wielokamerowymi systemami poprzez automatyczne poinformowanie operatora i administratora o utracie jakości obrazu.

Niezależnie od wyspecyfikowanych możliwości nadrzędnej platformy monitoringu, **uzgodniono instalację w modernizowanym budynku Zakładu Anatomii niezależnego rejestratora kompatybilnego z budowanym systemem i zintegrowanym z platformą VMS-CCTV**. Niezależnie od ilości projektowanych kamer w modernizowanym budynku, rejestrator powinien umożliwić obsługę do 64 kamer (dla możliwości włączenie kolejnych kamer z lokalnych zamierzeń inwestycyjnych).

3.1. Koncepcja dozoru wizyjnego

Przyjęto następujące założenia, stanowiące podstawę opracowania:

- instalacja dozoru wizyjnego ma na celu monitorowanie:
 - obszaru zewnętrznego
 - wejść do budynku (kamery dyskretne montowane na wysokości 150cm od posadzki dla bezproblemowego rozpoznania osób),
 - istotnych pomieszczeń i obszarów (serwerownia)
- system oparty o urządzenia (kamery, rejestratory) IP,

- zasilanie kamer z przełączników PoE,
- ochrona kamer zewnętrznych ochronnikami przeciwprzepięciowymi,
- stanowisko lokalnego monitorowania zlokalizowane w pomieszczeniu techników [K0/3],
- jako okablowanie sygnałowe zastosowane będą kable skrętkowe (projekt instalacji teletechnicznych).
- szafa dystrybucyjna oraz urządzenia w niej zlokalizowane będą zasilane z wydzielonych obwodów 230VAC [napięcie gwarantowane – projekt instalacji elektrycznych]

W tabeli poniżej przedstawiono zakres nadzorowania poszczególnych obszarów:

kamera	Lokalizacja	Scena obserwacji	Typ kamery	Kąt obserwacji
KAM-01	Elewacja zachodnia	południowa	Kamera bulet	Kąt obserwacji 70°
KAM-02	Elewacja zachodnia	Wejście do budynku	Kamera bulet	Kąt obserwacji 30°
KAM-03	Elewacja południowa	Wejście do budynku	Kamera bulet	Kąt obserwacji 50°
KAM-04	Elewacja południowa	zachodnia	Kamera bulet	Kąt obserwacji 50°
KAM-05	Elewacja wschodnia	północna	Kamera bulet	Kąt obserwacji 50°
KAM-06	Elewacja wschodnia	południowa	Kamera bulet	Kąt obserwacji 50°
KAM-07	Elewacja północna	zachodnia	Kamera bulet	Kąt obserwacji 50°
KAM-08	Elewacja zachodnia	południowa	Kamera bulet	Kąt obserwacji 30°
KAM-09	Wejście główne	identyfikacja	Kam. dyskretna	Kąt obserwacji 90°
KAM-10	Wejście główne	identyfikacja	Kam. dyskretna	Kąt obserwacji 90°
KAM-11	Wejście A1	identyfikacja	Kam. kopułkowa	Kąt obserwacji 30°
KAM-12	serwerownia	identyfikacja	Kam. kopułkowa	Kąt obserwacji 90°
KAM-13	Wejście B	identyfikacja	Kam. dyskretna	Kąt obserwacji 90°
KAM-14	Wejście B	identyfikacja	Kam. dyskretna	Kąt obserwacji 90°
KAM-15	Zadaszona pochylnia	północna	Kamera bulet	Kąt obserwacji 30°
KAM-16	Zadaszona pochylnia	południowa	Kamera bulet	Kąt obserwacji 30°

Identyfikacja, czyli rejestracja osób i przedmiotów z jakością kategorii I i II. (500-1000px/m) pozwalającą na ewentualne rozpoznanie osób czy przedmiotów, jeśli zajdzie taka potrzeba , ponadto dla takich kamer niezbędne będzie ustawienia większej ilości rejestrowanych klatek/s.

3.2. Struktura instalacji

Zgodnie z przyjętymi założeniami wstępnie zakłada się instalację następujących urządzeń:

- Kamery w obudowach zewnętrznych (odpornych na niekorzystne warunki środowiskowe) dla instalacji na zewnątrz budynku – mogą to być w zależności od możliwości montażowych kamery w obudowach typu bulet lub kopułkowe w obudowach wandaloodpornych.
- Kamery w obudowach kopułkowych w zależności od potrzeb wyposażone w oświetlacze IR dozoruujące wewnętrzne korytarze oraz pomieszczenia wewnątrz w budynku.
- Kamery dyskretnie montowane na wysokości 150cm dla celów identyfikacji osób wchodzących do budynku składające się z modułu terminala dla jednej lub dwóch kamer oraz wyniesionych miniaturowych obiektywów maskowanych dedykowanymi osłonami lub elementami wystroju wewnątrz.

- Rejestracja wizji odbywać się będzie na rejestratorze (serwerze) sieciowym, o wydajności dobranej odpowiednio dla oczekiwanego strumienia wizji z zaprojektowanych i przyszłych kamer oraz oczekiwanego czasu rejestracji dla zaproponowanego profilu rejestracji (jakość kompresji, ilości nagrywanych klatek/ sek, harmonogramy, detekcja ruchu, itp.)
- Monitorowanie lokalne na lokalnej stacji klienckiej w pomieszczeniu techników.
- Monitorowanie główne w pomieszczeniu ochrony PUM odbywać się będzie za pomocą dedykowanych istniejących wielomonitorowych stacji klienckich,
- 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,
- Dla kamer zewnętrznych montowanych na elewacji w pobliżu gniazd przyłączeniowych RJ45 sieci ethernet zaprojektowane zostaną w obudowach ochronnych ochronniki przeciwprzepięciowe dedykowane dla urządzeń CCTV, chroniące tory wizji i zasilania ograniczające przepięcia do poziomów poniżej 500V. Ponieważ projektowane kamery znajdują się w strefie ochronnej budynków należy zastosować ochronę przeciwko przepięciom atmosferycznym indukowanymi (prądy udarowe 8/20ms)
- 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].
- System dozoru wizyjnego będzie rozwiązaniem niezależnym od systemów miejskich/gminnych z opcją udostępniania im strumieni wideo lub oprogramowania klienckiego (za zgodą zarządzającego obiektem).

3.3. Dobór rozwiązań technicznych

Dobór kamer zostanie przeanalizowany po kątem oczekiwanej jakości rejestrowanego materiału wideo z obserwowanych scen.

Przy doborze kamer założono uzyskanie minimalnej jakości rejestrowanego obrazu pozwalające na późniejsze rozpoznanie przy jakościach (jeśli to technicznie możliwe) odwzorowujących obiekty o wysokości 1m na 100px rejestrowanego obrazu (kategoria 3) oraz 500px (kategoria 2) dla kamer służących do identyfikacji.

Dokonując wyboru lokalizacji kamer przyjęto dla kamer dozoru otoczenie budynku obserwację najbardziej odległej sceny z rozdzielczością umożliwiającą rozpoznanie (100px/1m), co dla kamer o rozdzielczościach co najmniej 4MPx pozwala na dozоровanie obszarów:

- przy kącie obserwacji ok. 30° w odległości do ok. 55m.
- przy kącie obserwacji ok. 50° w odległości do ok. 30m.
- przy kącie obserwacji ok. 70° w odległości do ok. 22m.
- przy kącie obserwacji ok. 90° w odległości do ok. 18m.

Kamery dozoru przejścia oraz pomieszczenia o ograniczonym dostępie pracować będą z obiektywami szerokokątnymi 30°-90°, co umożliwi identyfikację osób.

Kamery dyskretne dostępne są w ograniczonej ofercie z obiektywami stałymi umożliwiającymi identyfikację w kategorii II (obraz >500px/m), jednak z uwagi na przeciętne czułości oraz jasności obiektywów, wymagają dobrego oświetlenia sceny.

Zgodnie z przyjętymi założeniami wstępnie wytypowano lokalizację niezbędnych kamer, pozwalających na monitorowanie wcześniej zdefiniowanych newralgicznych rejonów. Lokalizację ka-

mer zaznaczono na podkładach budowlanych w części graficznej opracowania. Ilość typowych miejsc dozoru przedstawiono w tabeli w pkt. 3.1.

Kamery wewnętrzne montowane będą na sufitach i ścianach, kamery zewnętrzne (bulet) na elewacjach budynku.

Zgodnie z powyższym dla monitorowania założonych obszarów niezbędne jest zainstalowanie 16 kamer dla monitoringu wejść do budynku i jego otoczenia.

Dla projektowanych kamer przewidziano gniazda przyłączeniowe [projekt instalacji teletechnicznej].

Wizja z projektowanych kamer będzie rejestrowana lokalnie oraz docelowo w centralnym systemie rejestracji obrazu IP CCTV na serwerach i macierzach przewidzianych dla kompletnego systemu (budynek Kliniczno-Dydaktyczno-Badawczego PUM). Zainstalowany serwer umożliwi integrację instalacji lokalnej z instalacjami innych budynków wybudowanych i będących w realizacji.

Serwer lokalny w budynku Zakładu Anatomii zostanie zlokalizowany w serwerowni [-1.38]. [Przyjęto zgodnie z ustaleniami urządzenie rejestrujące do 64 strumieni wraz z dostępną \(po rozbudowie\) przestrzenią dyskową dla rejestracji wizji z 64 kamer \(wstępnie pojemność dostarczonych dysków powinna zapewnić rejestrację strumieni z projektowanych w budynku Anatomii kamer\).](#)

Dla monitorowania wewnętrznych i zewnętrznych stref w budynku zastosowano kamery o rozdzielczości 4Mpx/5Mpx, kamery dyskretne o rozdzielczości 2Mpx

Maksymalny strumień generowany przez te kamery dla kompresji H.264 przyjęto odpowiednio:

Dla kamer 2Mpx/ (5Mpx) przyjęto dla 6 kl/s strumień 2,5Mb/s / 6Mb/s

Dla kamer identyfikacyjnych rejestrujących obraz z jakością co najmniej II kategorii przyjęto

Dla kamer stacjonarnych 2Mpx przyjęto dla 12 kl/s strumień 5Mb/s

Przyjęte strumienie są orientacyjne, ponieważ silnie zależą od zmian w dozoru scenach oraz ustawień parametrów rejestracji wybranych kamer

Kamery zainstalowane w budynku Zakładu Anatomii wykorzystywane będą głównie podczas codziennej pracy, przyjęto szybkość rejestracji 6kl/s. Strumień generowany przez te kamery dla kompresji H,264 oraz niezbędną przestrzeń dyskową przedstawiono poniżej:

kamera	fps	kodek	nagrywanie	det.ruchu	bitrate	czas rejestracji	dysk	ilość kamer	bitrate	dysk
kategoria III										
5Mpx	6kl/s	H.264	ciągłe	30%	6,0Mb/s	24godz	0,019TB	12	72,0Mb/s	0,233TB
ilość dni archiwizacji								1	72Mb/s	0,23TB
kategoria I / II										
2Mpx	12kl/s	H.264	ciągłe	50%	5,0Mb/s	24godz	0,027TB	4	20,0Mb/s	0,108TB
ilość dni archiwizacji								1	20Mb/s	0,11TB
RAZEM								1	92Mb/s	0,34TB
archiwizacja								30	dni	10TB

Dla budynku Zakładu Anatomii przyjmuje się 30 dni dla przechowywania materiałów archiwalnych, wymagana przestrzeń dyskowa wyniesie ok. 10TB, dla pozostałych wolnych kanałów rejestracji łączna przestrzeń dyskowa powinna być nie mniejsza niż 40TB

Aby zapewnić rezerwę dla różnic wynikających z warunków panujących w obiekcie oraz dla realizacji konfiguracji RAID należy przyjąć dyski o pojemności 5x 12TB ([w pierwszym etapie 2x12TB](#)).

3.4. Dobór urządzeń

3.4.1. Kamera 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: Poziomo: 100°(Wide) ~ 33°(Tele)
- Obiektyw autoiris, sterowany zdalnie, ogniskowa 2,7-13mm, mechaniczny filtr IR
- czułość (bez IR) wymagania minimalne: kolor 0,003lux / F1,4
- Dynamika 120db
- IK10 oraz IP67
- Zasilanie 12Vdc, PoE IEEE 802.3at (max.13,6W)
- Temperatura pracy -30 C..+50 C

3.4.2. Kamera stacjonarna wewnętrzna

- Kamera kopułowa wandaloodporna
- Rozdzielczość min: 2 Mpx
- Kompresja MJPEG, H.264 oraz H.265
- Prędkość odświeżania 30 kl/s
- Minimalne kąty widzenia: Poziomo : 100°(Wide) ~ 33°(Tele)
- Obiektyw autoifis, ogniskowa 3,2-10mm, mechaniczny filtr IR
- czułość (bez IR) wymagania minimalne: kolor 0,03lux / F1,6
- Dynamika 120db
- IK10 oraz IP66.
- Zasilanie 12Vdc, PoE IEEE 802.3af (max.7,7W)
- Temperatura pracy -30 C..+50 C

3.4.3. Kamera dyskretna wewnętrzna

- Kamera składająca się z modułu terminala i wyniesionych obiektywów dyskretnych
- Rozdzielczość min: 2 Mpx
- Kompresja MJPEG, H.264 oraz H.265
- Prędkość odświeżania 60 kl/s
- Minimalne kąty widzenia: Poziomo: 73° (ogniskowa 4,6mm)
- Obiektyw o stałej ogniskowej 4,6mm
czułość wymagania minimalne: kolor 0,06lux / F2,5
- Dynamika 120db
- Zasilanie 12Vdc, PoE (max.6,5W)
- Temperatura pracy -10 C..+50 C

3.4.4. Rejestracja wizji

Rejestrator IP dla rejestracji strumieni wideo, spełniający następujące warunki:

- Rejestratory powinny obsługiwać tryb failover, tj. w przypadku awarii rejestratora automatycznie jego rolę powinien przejąć rejestrator zapasowy
- Nieodpłatne licencje klienckie
- 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

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.
- Obsługa następujących formatów: MJPEG, MPEG-4 SP, MPEG-4 ASP, MxPEG , H.264 oraz H.265
- Obsługa 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 zakładek 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

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

- Obudowa rack,
- Kieszenie dla 8 dysków HDD,
- Konfiguracja RAID-5,
- system operacyjny Win 10 Pro 64-bit
- pamięć RAM min.16GB
- procesor serii Intel XENON E2, lub równoważny
- karta sieciowa 4x 1Gb
- dysk SSD (SATA III min.128GB)
- klawiatura, mysz optyczna USB
- zasilanie 230V / 650W redundantne
- temperatura pracy 5°C - 40°C

Rejestracja wizji odbywać się będzie na dyskach HDD serwera systemu CCTV. Dla projektowanego systemu licencją objęte są serwery i przyłączane kamery, dla zarządzania instalowanymi urządzeniami należy wdrożyć platformę zarządzania obrazem, to jest oprogramowaniem serwera master i redundantnego slave działających w trybie klastrowym, integrującym również systemy KD, SWiN, interkomowy. Oprogramowanie dostarczane jest jako licencje na zamówione moduły według potrzeb. W przypadku zarządzania obrazem licencje dotyczą ilości obsługiwanych

nych kamer, wspieranych serwerów, kanałów video i ostatecznie będzie zależać od projektu kompletnego systemu.

Do wybranej wersji oprogramowania trzeba dołożyć odpowiednią ilość licencji podłączanych urządzeń oraz wymaganych niestandardowych funkcjonalności (integracje, analiza obrazu).

3.4.5. Prezentacja wizji

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 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, wyzwalanie 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 wyzwalania zaawansowanych makr oferujących możliwość wielopoziomowych akcji, w tym min wysterowanie presetów kamery PTZ, aktywacja wyjścia przekątnikowego 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 otwarcie 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 nagrywania 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 metadaniem 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 odroczonego 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 będą 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 ty-

pu 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 dołączonym 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, analizy twarzy, detekcji twarzy, detekcji koloru, zakładek z komentarzem operatora oraz innych zdarzeń występujących w systemie VMS za pomocą prążków, po najechaniu 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

3.4.6. Ochronnik przeciwprzepięciowy

Dla urządzeń zewnętrznych montowanych na elewacji w pobliżu gniazd przyłączeniowych RJ45 sieci ethernet należy umieścić w obudowie ochronnej ochronnik przeciwprzepięciowy chroniących tory wizji i zasilania ograniczające przepięcia do poziomów poniżej 500V. Jeśli to możliwe, puszkę z ochronnikami należy montować w miejscu wykonania przewiertu przez ścianę lub w sąsiedztwie takiego przewiertu.

Ponieważ projektowane urządzenia znajdują się w strefie ochronnej budynków należy zastosować ochronę przeciwko przepięciom atmosferycznym indukowanymi (prądy udarowe 8/20ms).

Ochrona toru ethernet PoE [wymagania minimalne]:

- Kategoria ochrony C1/D1
- znamionowy prąd wyładowczy 2,5kA (8/20ms),
- maksymalny prąd piorunowy 1kA (10/350ms),
- największe napięcie trwałej pracy 60Vdc
- częstotliwość graniczna 250MHz (3dB)
- Gniazda RJ 45 obustronne kat.6,
- Przeznaczony dla kabli ekranowanych i nieekranowanych

3.5. 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 obiektywów 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.

3.6. Zasilanie systemu monitoringu wizyjnego

Zasilanie kamer z przełączników sieciowych PoE [projekt instalacji teletechnicznej]

Przełączniki sieciowe zainstalowane w szafach teletechnicznych będą zasilane z zasilacza za pośrednictwem listwy zasilającej.

Zasilanie 230V zgodnie z projektem instalacji elektrycznej

3.7. Zestawienie materiałów - CCTV

Opis materiałów	mod.referencyjny	ilość
URZĄDZENIA		
Kamera zewnętrzna "bulet" 5Mpx	[wg specyfikacji]	12
Kamera kopułkowa wandaloodporna 2Mpx	[wg specyfikacji]	2
Mkamera dyskretna 2Mpx	[wg specyfikacji]	4
rejestrator IP rejestracja min 64 strumieni	[wg specyfikacji]	1
Oprogramowanie zarządzające- licencja podstawowa	[wg specyfikacji]	1
licencja dla kanału wizyjnego	[wg specyfikacji]	16
Dysk HDD 12TB		2
stacja operatorska	[wg specyfikacji]	1
monitor LCD 27"	[wg specyfikacji]	1
ogranicznik przepięć PoE	[wg specyfikacji]	8
obudowa izolacyjna ogranicznika przepięć		5

4. INSTALACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM - SMS

4.1. Uwarunkowania wstępne projektowanego systemu

Uwzględniając politykę bezpieczeństwa Pomorskiego Uniwersytetu Medycznego w Budynku Kliniczno-Dydaktyczno-Badawczym przy ulicy Unii Lubelskiej zaprojektowano system bezpieczeństwa SMS mający za zadanie zarządzać, sterować, optymalizować działania, w szczególności następujących systemów:

- system kontroli dostępu (KD)
- system dozoru telewizyjnego przemysłowej (CCTV)
- system wykrywania i sygnalizacji włamania (SSWiN)
- system wykrywania i sygnalizacji pożaru (SAP)
- system automatycznego gaszenia pożaru (SAG)
- 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 umożliwia wzajemne współdziałanie poniższych podsystemów za pomocą interfejsów programowych:

- Kontroli Dostępu,
- Sygnalizacji Włamania i Napadu
- Monitoringu Wizyjnego CCTV IP
- Interkomowego
- iManager
- Zarządzania kluczami – depozytor kluczy
- Sygnalizacji Pożarowej
- iSRS (System Zarządzania Sal)
- ProAkademia

Platforma SMS umożliwia zdalną diagnostykę (przez sieć Internet) i lokalną przez komputer w sieci, lub komputer podłączony do sterownika systemu KD z hiperterminalem.

Nieależnie 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 jest 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 informacje 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).

Platforma SMS umożliwia pełne raportowanie i archiwizację danych. System ma 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 umożliwia 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.

System musi mieć wbudowaną mapę synoptyczną (wizualizację) dla każdego nadzorowanego obiektu, 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 sygnalizacji zagrożenia pożarem - wizualizacja na mapie synoptycznej stanu poszczególnych detektorów i/lub stref SSP.

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, czy rozpoznawania twarzy z systemem kontroli dostępu. Numer rejestracyjny lub wzór twarzy 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.

Platforma SMS musi mieć także możliwość realizacji następujących funkcjonalności między-systemowych:

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.

Elementami wykonawczymi platformy SMS muszą być:

- inteligentne sterowniki sieciowe pozwalające na podłączenie elementów wykonawczych systemów Kontroli Dostępu, SSWiN,
- komunikacja sieciowa
- serwer

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 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.

4.2. Projektowana realizacja uwzględniająca strategię Inwestora

W trakcie uzgadniania sposobu integracji systemów zabezpieczeń technicznych przewidziano instalację serwera Security Managment System wraz z systemem kontroli dostępu w projektowanym Budynku Kliniczno-Dydaktyczno-Badawczym przy ulicy Unii Lubelskiej.

W przypadku rozbudowy systemu KD i podłączania kolejnych budynków do systemu Kontroli Dostępu na PUM, główny serwer będzie dalej zlokalizowany na Budynku Kliniczno-Dydaktyczno-Badawczym przy ulicy Unii Lubelskiej z redundancją COLD STAND-BY na Międzywydziałowym Centrum Dydaktyki nr 3 przy ul. Unii Lubelskiej.

Nie przewiduje się projektowania kolejnych serwerów.

5. INSTALACJA SYSTEMU KONTROLI DOSTĘPU – SKD

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

System KD musi spełnić wymogi klasy dostępu B i klasy rozpoznania 3.

5.1. Koncepcja sterowania dostępem

Przyjęto następujące założenia, stanowiące podstawę opracowania:

- należy nadzorować trzy wejścia do budynku, zgodnie z uzgodnieniami elementami blokującymi mają być zwory elektromagnetyczne
- należy nadzorować dostęp do pomieszczenia serwerowni, zgodnie z uzgodnieniami wymagana kontrola dwustronna
- należy nadzorować dostęp do pomieszczeń socjalnych i do szatni, (kontrola jednostronna, element wykonawczy elektrozaczep NO),
- należy nadzorować dostęp do gabinetów pracowników dydaktycznych, (kontrola jednostronna, element wykonawczy elektrozaczep NO)

Łącznie wytypowano 19 nadzorowanych systemem KD przejść oraz jedno nadzorowane systemem SWiN wyjście awaryjne.

na wytypowanych przejściach zainstalowane zostaną zgodnie z ustaleniami następujące urządzenia:

- czytnik kart,
- przycisk wyjścia,
- przycisk ewakuacyjny,
- zwora elektromagnetyczna lub elektrozaczep rewersyjny,
- samozamykacz,
- zestaw klamka – klamka

Urządzenia systemu KD nadzorowane będą przez kontrolery zainstalowane w szafie KD w pomieszczeniu serwerowni.

5.2. Dobór zastosowanych rozwiązań – system SKD

Biorąc pod uwagę przyjęty w budynkach PUM standard, zdecydowano o wyborze czytników i kart pracujących w standardzie MIFARE. 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 rozwijowanym systemem centralnego zarządzania wdrażanym w istniejących i realizowanych w obiektach PUM.

5.2.1. czytnik zbliżeniowy,

- Wspieranie technologii: Mifare,.

- Montaż natynkowy i podtynkowy, czytniki w wersji podtynkowej – montaż w standardowej elektrycznej puszcze podtynkowej,
- Wszystkie elementy elektroniczne czytnika wewnątrz obudowy zalane żywicą epoksydową,
- Temperatura pracy $-35^{\circ}\text{C} \dots +65^{\circ}\text{C}$,
- Stopień ochrony IP54

5.2.2. kontroler KD,

Czytniki kart zbliżeniowych dla podwyższenia bezpieczeństwa systemu współpracują z niezależnymi kontrolerami, sterującymi elementami wykonawczymi (rygle, elektrozawory, 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 przekaźnikowe – 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 $-35^{\circ}\text{C} \dots +65^{\circ}\text{C}$,

5.2.3. 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

5.2.4. Przycisk wyjścia

Przycisk umożliwiający wyjście z pomieszczenia z jednostronna kontrolą dostępu przy zastosowaniu elektrozawory lub elektrozaczepu instalowanego w drzwiach pożarowych (montaż z dodatkowym przeciwwzamkiem).

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

5.2.5. 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,

5.2.6. 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,

5.2.7. Elementy wykonawcze,

- zwory elektromagnetyczne – elementy dostarczane ze stolarką drzwiową, w wykonaniu NO (rewersyjnym) z zasilaniem 12V DC.
- Zwora wyposażona w czujnik domknięcia drzwi,

5.2.8. Elementy wykonawcze,

- elektrozaczepty – elementy dostarczane ze stolarka drzwiową, w wykonaniu NO (rewersyjnym) z zasilaniem 12V DC.
- elektrozaczepty wyposażony w styk dozoru domknięcia drzwi,

5.2.9. Zasilacze buforowe,

- Zasilacz impulsowy,
- Akumulatory rezerwowe umożliwiające do 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, przeciwzwarcowe, przeciwprzeciążeniowe, przeciw odwrotnym podłączeniem i rozładowaniem akumulatora,
- Sygnalizacja (wyjście przekaźnikowe) stanu zasilania podstawowego oraz niskiego stanu akumulatora,

5.2.10. Oprogramowanie zarządzające systemem KD

Poniżej zawarto opis funkcjonowania wdrażanego systemu w budynkach Pomorskiego Uniwersytetu Medycznego, którego wymagania powinny spełniać projektowane nowe systemy zabezpieczeń technicznych.

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

Wirtualizacja

Biorąc pod uwagę Wieloletnią Koncepcję Rozwoju Systemów Bezpieczeństwa na PUM projektowany system bezpieczeństwa musi umożliwiać wirtualizację, Dlatego system bezpieczeństwa musi się cechować następującymi możliwościami:

- System KD musi posiadać wsparcie i możliwość instalacji w środowisku wirtualnym.
- Minimalne wymagania to wsparcie i możliwość instalacji serwera KD:
 - w środowisku VMware
 - w środowisku Hyper-V
 - Active Directory (AD).

Biorąc pod uwagę Wieloletnią Koncepcję Rozwoju Systemów Bezpieczeństwa na PUM projektowany system bezpieczeństwa musi umożliwiać wykorzystanie Active Directory (AD). Dlatego system bezpieczeństwa musi się cechować następującymi możliwościami:

- System KD musi zapewniać możliwość synchronizacji użytkowników oraz uprawnień z systemem nadrzędnym Active Directory (AD).

- Na podstawie informacji z AD dane użytkowników w SKD muszą być aktualizowane automatycznie w ważność ich dostępu odpowiednio modyfikowana
- Aktywacja lub dezaktywacja konta w AD musi powodować odpowiednio przyznanie lub zablokowanie ważności kart w SKD
- Zmiana danych (imienia lub nazwiska) w AD musi zmienić dane powiązanego użytkownika w SKD pozostawiając jednocześnie jego uprawnienia.
- Usunięcie użytkownika AD musi spowodować wyłączenie wszystkich kart danej osoby w SKD.
- Dodanie nowego użytkownika w AD musi spowodować utworzenie nowej osoby w SKD bez przypisanych kart.
- Synchronizacja SKD z AD musi umożliwiać synchronizację uprawnień dostępu do czytników/grupy czytników

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

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 dostępową 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

Serwer systemowy

Serwer z oprogramowaniem licencjonowanym dla zainstalowanej ilości przejść i użytkowników. jest zlokalizowany w Budynku Kliniczno-Dydaktyczno-Badawczym przy ulicy Unii Lubelskiej Serwer po zainstalowaniu odpowiednich licencji pozwoli na administrowanie systemem KD oraz na integrację systemów SWiN, KD, CCTV projektowanego budynku oraz innych budynków wybudowanych i będących w realizacji.

Administracja systemem

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 ProAkdemia,
- 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 ProAkademia

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 ProAkademą 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 funkcjonowania, wdrażany w budynkach:

- w Międzywydziałowym Centrum Dydaktyki nr 3,
- w Centrum Symulacji Medycznych,
- w Budynku Kliniczno-Dydaktyczno-Badawczym ,

W projektowanym Budynku Katedry Anatomii przy ul. Powstańców Wielkopolskich wymagane jest wdrożenia opisanych funkcjonalności.

5.2.11. Karty bezstykowe autoryzacji dostępu

W systemie będą używane karty bezstykowe MIFARE.

5.2.12. Okablowanie

Przewody powinny spełniać wymogi rozporządzenia CPR:

- okablowanie budynku poza drogami ewakuacyjnymi. kl. CPR Dca-s1b,d2,a1)
- okablowanie przebiegającego przez drogi ewakuacyjne kl. CPR B2 ca s1 d1 a1)

wymogi takie spełniają między innymi przewody:

okablowanie czytników - skrętka ekranowana typu CAT6A STP,

okablowanie zamków elektrycznych, kontaktronów, czujników - skrętka typu HTKSH 4x2x0,8,

5.3. Bilans energetyczny

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 $k=1,25$

I_1 – całkowity prąd dozoru

I_2 – całkowity prąd alarmowania/ sterowania

t_1 – czas dozoru – wymagany czas dozoru,

t_2 – 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 2 kontrolerów (maksymalnie 4 nadzorowane przejścia) oraz jednego kontrolera sieciowego (GRADE 3) oraz
- do 4 kontrolerów (8 nadzorowanych przejść) oraz jednego kontrolera sieciowego (GRADE 2).

dla zasilania grupy kontrolerów obsługujących 4 przejścia przewidziano jeden zasilacz buforowy

dla zasilania grupy kontrolerów obsługujących 8 przejść przewidziano jeden zasilacz buforowy

GRADE 3			
kontroler sieciowy	0,208 A	1 szt.	0,208 A
kontroler drzwiowy	0,040 A	2 szt.	0,080 A
czytnik kart	0,058 A	4 szt.	0,233 A
elektrozwoła	0,320 A	4 szt.	1,280 A
akumulator 17Ah		1 szt.	
zasilacz 12V/7A			
razem:			1,802 A

GRADE 2			
kontroler sieciowy	0,208 A	1 szt.	0,208 A
kontroler drzwiowy	0,040 A	4 szt.	0,160 A
czytnik kart	0,058 A	8 szt.	0,467 A
elektrozwoła	0,320 A	8 szt.	2,560 A
akumulator 17Ah		1 szt.	
zasilacz 12V/7A			
razem:			3,395 A

dobór wymaganego źródła zasilania awaryjnego:

$$C_{\min} = 1,25 \times (A_1 \times t_1 + A_2 \times t_2)$$

t_1 (minimalny czas czuwania)= 4 h

$C_{\min} = 9,59 \text{ Ah}$

zastosowano akumulator o pojemności $C_{\text{nom}} = 18,00 \text{ Ah}$

przewidywany czas pracy awaryjnej: $t_1 = 7,74 \text{ h}$

dobór wymaganego źródła zasilania awaryjnego:

$$C_{\min} = 1,25 \times (A_1 \times t_1 + A_2 \times t_2)$$

t_1 (minimalny czas czuwania)= 2 h

$C_{\min} = 9,56 \text{ Ah}$

zastosowano akumulator o pojemności $C_{\text{nom}} = 18,00 \text{ Ah}$

przewidywany czas pracy awaryjnej: $t_1 = 3,99 \text{ h}$

5.4. Struktura sieciowa instalacji KD

Zaprojektowane urządzenia budynkowej kontroli dostępu przedstawiono w tabeli poniżej, zgodnie z listą kontrolerów sieciowych:

gniazdo eth	kontroler sieciowy	ilość kontrolerów	ilość czytników	przyciski EWAK	przyciski wyjścia	elektro zwora	elektrozaczep NO	moc zasilania	lokalizacja
ETH#1	1	2	4	4	2	3	1	60 W	serwerownia
ETH#2	1	4	8				8	60 W	serwerownia
ETH#3	1	4	8				8	60 W	serwerownia
razem	3	10	20	4	2	3	17		

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

- Kontrolery sieciowe 3 szt
- Kontrolery drzwiowe 10 szt
- Czytniki bezstykowe 20 szt
- Zwory elektromagnetyczne z kontrolą domknięcia 3 szt
- Elektrozaczepy rewersyjne z kontrolą domknięcia 17 szt
- Przyciski wyjścia 2 szt
- Przyciski ewakuacyjne z podwójną parą styków 4 kpl

Urządzenia zasilane z trzech zasilaczy o mocach 60W z baterią akumulatorów 18Ah'

5.5. Zestawienie materiałów - SKD

czytnik kart bezstykowych		20 szt
karta bezstykowa		100 szt
przycisk wyjścia		2 szt
przycisk ewakuacyjny (2 kpl styków NC/NO)		4 szt
oprogramowanie zarządzające systemem KD, SWiN - licencje:		
rozszerzenia - dodatkowy operator		1 kpl
rozszerzenie - dodatkowy czytnik		20 kpl
rozszerzenie - obsługa map		1 kpl
rozszerzenie - integracja z centralą SWiN		1 kpl
rozszerzenie - integracja z 1 kamerą		16 kpl
rozszerzenie - dodatkowy monitor SRS		3 kpl
stacja operatorska [mysz , klawiatura]	[wg specyfikacji]	1 kpl
monitor LCD 27"	[wg specyfikacji]	1 kpl
zasilacz 12V/5A		3 szt
akumulator 12V/18Ah	EP17	3 szt
szafa stalowa z zamkiem, styki sabotażowe otwarcia i odrywania od podłoża, profile monrażowe TH35, 600x500x200,		2 kpl
elektrozaczep 12V NO z monitoringiem domknięcia	[dostawa z drzwiami]	17 szt
elektrozwoz 12V NO z monitoringiem domknięcia	[dostawa z drzwiami]	3 szt
OKABLOWANIE SYSTEMU		
przewód UTP 4x2x0,5		600 mb
przewód LiHH 6x0,75		600 mb
przewód LgY6		200 mb
rurka instalacyjne sztywna samogasnąca PCV fi 25		
rurka instalacyjne giętka samogasnąca PCV z pilotem fi 25		150 mb

6. INSTALACJA SYSEMU INTERKOMOWEGO

W projektowanym budynku Katedry Anatomii przewiduje się montaż prostego systemu interkomowego umożliwiającego łączność pomiędzy dwoma wejściami do budynku z drzwiami objętymi systemem KD, a pomieszczeniem techników, pomieszczeniami socjalnymi oraz kilkoma innymi wskazanymi lokalizacjami.

Zgodnie z przyjętym standardem w budynkach PUM należy zastosować urządzenia typu master-slave z sześcioma stacjami odbiorczymi oraz modułem GSM dla przekierowywania rozmowy na telefon.

6.1. Dobór zastosowanych rozwiązań – system interkomowy

Dla zdefiniowanej wyżej struktury przewidziano instalację urządzeń cyfrowych z komunikacją dwuprzewodową i osobną linią sterującą urządzenia aktywne poprzez wejścia kontrolerów KD.

Z uwagi na strukturę systemu obejmującego:

- kilka niezależnych wejść,
- konieczność dzwonienia z wejść tylko na dwa równorzędne odbiorniki,
- oraz wybrany typ instalacji (dwuprzewodowy) z gwiazdzystym okablowaniem urządzeń,

należy strukturę instalacji połączyć w następujący sposób:

- w pierwszej kolejności wszystkie panele wejściowe szeregowo w układzie master / slave / slave.../ slave,
- następnie wszystkie odbiorniki szeregowo odpowiednio adresując odbiorniki, tak, aby aparat nadrzędny, do którego będzie można dzwonić ze wszystkich paneli wejściowych był przypisany do tego samego klawisza wywołania w panelach wejściowych.
- Ponadto w module master należy zainstalować moduł GSM umożliwiający przekierowanie wywołań na zaprogramowane numery telefonów.

6.1.1. Panel przywoławczy systemu cyfrowego,

- Montaż podtynkowy, dostępna puszka dla montażu natynkowego,
- Płaski panel przedni, przyciski ze stali nierdzewnej szczotkowanej,
- Modele 1-przyciskowy, 2-przyciskowy,
- Indywidualnie podświetlany przycisk wywołania,
- Typ instalacji – cyfrowa 2-żyłowa (długość linii do 300m dla przewodów 0,5mm)
- Zasilane 15VDC (nie stosować zasilania AC)
- Dostępne wyjścia sterowania elektrozaczepu beznapięciowe typu NO/NC (dopuszcza się wykorzystanie systemowych modułów przekaźnikowych)
- Akustyczna i optyczna sygnalizacja funkcji panelu,
- Możliwość podłączenia dodatkowego sygnalizatora akustycznego lub optycznego wspomagające dzwonienie odbiornika,
- Możliwość podłączenia wielu odbiorników pod jednym numerem wywołania,
- Indywidualne ustawianie parametrów dźwiękowych,
- Obsługa wielowejsściowych systemów master / slave,
- Współpraca z modułami GSM,
- Temperatura pracy -20°C...+50°C,

6.1.2. Odbiornik interkomu,

- Unifon bezsłuchawkowy i
- Unifon aktywny z funkcją dzwonka do drzwi
- Obudowa ABS,
- Zasilanie 15V DC
- Typ instalacji – cyfrowa 2-żyłowa + zasilanie DC
- Podłączenie magistrali – gniazdo RJ45
- Wielostopniowa regulacja natężenia dźwięku,
- Możliwość pracy kilku odbiorników na tym samym adresie,
- Funkcja dzwonka do drzwi (RING),
- Optyczna sygnalizacja dzwonienia,

6.1.3. Filtr przeciwzakłóceńowy.

- Filtr dedykowany dla instalacji zasilanych zasilaczy nieposiadających zacisku PE,
- Ogranicza pojawianie się przydźwięku i innych zakłóceń sygnału audio,
- Zalecany do instalacji z urządzeniami głośnomówiącymi,

6.1.4. zasilacz,

- Zasilacz 15Vdc/60W
- Montaż na szynie TE35

6.2. Wytyczne montażowe

- Instalacja na bazie tras kablowych instalacji niskoprądowych zabezpieczeń technicznych,
- Okablowanie instalacji interkomowej wykonać przewodem miedzianym 4x2x0,8.
- 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.

6.3. Zestawienie materiałów - INTERKOMY

Opis materiałów	model referencyjny	ilość
SYSTEM INTERKOMÓW CYFROWYCH 2-przewodowych		
Panel przywoławczy cyfrowy 2-żyłowy,		2 szt
unifon głośnomówiacy, aktywny, 2-żyłowy		6 szt
moduł GSM		1 szt
zasilacz panela przywoławczego		1 szt
filtr przeciwzakłóceńowy		1 szt
OKABLOWANIE SYSTEMU		
przewód UTP 4x2x0,5		300 mb
rurka instalacyjne PCV	RL25, RL28	60 mb

7. INSTALACJA SYSTEMU SYGNALIZACJI WŁAMANIA SWiN

7.1. 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 drzwiach oraz innych czujników wykrywających zagrożenia włamaniem (czujniki inercyjne) oraz zagrożenia techniczne (np. zalenie 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 [w [Budynku Kliniczno-Dydaktyczno-Badawczym PUM przy ul. Unii Lubelskiej](#)].
- 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.

7.2. 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 (serwerownia),
- podział na partycje (niezależnie uzbrajane) uwzględni:
 - wydzielone obszary zakładu anatomii,
 - wejścia do budynku
 - 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.

7.3. Dobór zastosowanych rozwiązań – system SWiN

7.3.1. 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 zabrania i rozbrajania stref podlegających ochronie za pomocą czytników kart.

Z uwagi na zakres przewidywanych stref ochrony należy wybrać centrale umożliwiającą późniejszą rozbudowę systemu SWiN o zmieniające się wymagania strefowania ochrony budynku:

- możliwość wydzielenie do 32 niezależnych stref ochrony,
- wielopoziomowa hierarchia kodów dostępu,
- zgodność z wymaganiami normy PN-EN 50131 Grade 3
- zabrania, 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

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

7.3.2. koncentrator i klaster central alarmowych

Centrala alarmowa musi zapewniać możliwość pracy w klastrze wielu central alarmowych (dla przyszłej integracji planowanych instalacji zabezpieczeń technicznych w innych sąsiednich obiektach)

Praca central alarmowych w klastrze musi umożliwiać użycie dedykowanego manipulatora klastrowego, z którego można obsługiwać wiele central alarmowych

Połączenie central alarmowych (klastrow) i manipulatorów klastrowych musi odbywać się pomocą koncentratora central alarmowych.

Do koncentratora można podłączyć:

- Do 8 manipulatorów klastrowych za pomocą magistrali RS-485

- Do 8 central alarmowych:
 - Każda centrala alarmowa musi komunikować się z koncentratorem za pomocą magistrali RS-485.
 - Pojedyncza centrala alarmowa pracująca w klastrze może obsłużyć do 512 wejść

Pojedynczy manipulator klastrowy może obsłużyć:

- 8 central alarmowych
- Do 4096 wejść
- Do 256 stref alarmowych
- Musi umożliwiać uzbrojenie i rozbrojenie stref
- Musi umożliwiać blokowanie i odblokowywanie wejść (bypass/omijanie)
- Otrzymywać powiadomienie ze wszystkich central alarmowych

Koncentrator musi obsługiwać centrale alarmowe działające w architekturze redundantnej złożonej z centrali master i slave. System musi umożliwiać wykonanie architektury z redundantnym koncentratorem. Architektura redundantnego koncentratora musi składać się z:

- Dwóch koncentratorów
- Koncentratory muszą być połączone za sobą za pomocą magistrali RS-485 dedykowanej dla koncentratorów
- Centrale alarmowe (klastry) muszą być podłączone na osobnej magistrali RS-485 do obydwóch koncentratorów

Jeden z koncentratorów musi być skonfigurowany jako koncentrator podstawowy (master), drugi koncentrator musi być skonfigurowany jako koncentrator redundantny (slave)

7.3.3. Szyfrator OLED

Klawiatura OLED umożliwiająca 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 konfigurację z 5 stopniową parametryzacją (N.O., N.C., EOL, AM, Fault)

Manipulator musi występować w 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 pracujący 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

7.3.4. Expander wejść/wyjść z zasilaczem

Pojedynczy expander z zasilaczem musi obsłużyć 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 dopuszczane 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 obsłużyć do 10 wyjść

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

7.3.5. Czujniki kontaktronowe

- Czujniki otwarcia drzwi lub okien osiowe, dostarczane łącznie z kompletną stolarką.
- 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

7.3.6. 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

7.3.7. 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

7.3.8. Detektory uderowy (inercyjny)

- Monitorowanie ataków z użyciem narzędzi mechanicznych,
- Detektor wibracyjny, 3 kanały wykrywania
- Promień ochrony do 3m
- Regulowana czułość
- Temperatura pracy -30°C... +55°C
- Zasilanie 12V dc,
- Czujnik spełniający normę EN50131-2-8 Grade 3

7.3.9. 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

7.3.10. Sygnalizator optyczno-akustyczny

- Sygnalizator zewnętrzny,
- Natężenie dźwięku na poziomie 120dB w odległości 1m
- Obudowa wykonana z odpornego na uderzenia i promieniowanie UV poliwęglanu lub ze stali nierdzewnej

7.4. Bilans energetyczny

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

Lokalizacja	Nr.pom.	Moduł we/wy z zasilaczem	Linie dozоровe	Moc zasilania	Uwagi
serwerownia	[x/x]	SWiN#00 SWiN#01 SWiN#02 SWiN#03	LD_001...128	4x60W	ethernet

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 dla $t=72h$, $k=1,25$ dla modułów alarmowych

I_1 – całkowity prąd dozoru

I_2 – całkowity prąd alarmowania/ sterowania

t_1 – czas dozoru – wymagany czas dozoru,

t_2 – czas alarmowania / sterowania równy 0,5h

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

7.5. 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 podciągi wykonać techniką bezударową - otwory $\phi 30$ 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.

7.6. Zestawienie materiałów – SWiN

Opis materiałów	uwagi	ilość
URZĄDZENIA		
centrala alarmowa (do łączenia w klastry) 128 linii dozorowych, zasilacz 8 wejść na płycie głównej		1 szt
moduł rozszerzenia z zasilaczem, 8 wejść na płycie głównej		3 szt
moduł rozszerzenia o 8 wejść,		10 szt
szyfrator graficzny OLED		2 szt
akumulator 12V/17Ah		4 szt
detektor ruchu PIR, Grade 3		37 szt
detektor ruchu PIR+MV, Grade 3		5 szt
detektor ruchu sufitowy		5 szt
czujnik inercyjny		24 szt
czujnik zalania wodą		1 szt
czujnik kontaktronowy osiowy, Grade 3		30 szt
puszka połączeniowa ze stykami sabotażowymi		30 szt
sygnalizator akustyczny zewnętrzny		1 szt
OKABLOWANIE SYSTEMU		
przewód typu UTP4x2x0,5		3700 mb
rurka instalacyjne PCV	RL25, RL28	400 mb
rurka instalacyjne peszla	16mm	3000 mb

7.7. Okablowanie instalacji niskoprądowych

Zgodnie z dyrektywą CPR i normą PN-EN 50575 w projektowanych instalacjach stosowane będą przewody i kable spełniające następujące warunki:

- dla okablowania prowadzonego na drogach ewakuacyjnych klasy reakcji na ogień co najmniej B2ca-s1b, d1,a1
- dla okablowania prowadzonego poza drogami ewakuacyjnymi klasy reakcji na ogień co najmniej Dca-S2, d1, a2,

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.

B. CZĘŚĆ GRAFICZNA

PW-N.ZT-01	Plan instalacji zabezpieczeń technicznych KD, SWiN, CCTV, INT - Poziom -1
PW-N.ZT-02	Plan instalacji zabezpieczeń technicznych KD, SWiN, CCTV, INT - Poziom 0
PW-N.ZT-03	Plan instalacji zabezpieczeń technicznych KD, SWiN, CCTV, INT - Poziom +1
PW-N.ZT-04	Schemat instalacji SWiN
PW-N.ZT-05	Schemat instalacji KD
PW-N.ZT-06	Schemat instalacji TVD