



44-330 Jastrzębie Zdrój, ul. Kasztanowa 60
tel: 511-695-121, 4matbiuro@gmail.com
NIP: 633-176-33-38
www.4mat.net.pl
REGON: 242910306
ING: 09 1050 1403 1000 0091 2528 9224

FIRMA PROJEKTOWO-WYKONAWCZA

PROJEKT ARCHITEKTONICZNO-BUDOWLANY

Modernizacja serwerowni wraz z instalacją strukturalną, dedykowaną instalacją elektryczną wewnątrz budynku Urzędu Miejskiego w Paczkowie

INWESTOR	Gmina Paczków, ul. Rynek 1, 48-370 Paczków
OBIEKT	Budynek Administracyjny
ADRES	Urząd Gminy Paczków, ul. Rynek 1, 48-370 Paczków

BRANŻA ARCHITEKTONICZNA	<u>PROJEKTANT</u> mgr inż. arch. Arkadiusz Zientala uprawnienia nr 21/99 w specjalności architektonicznej	mgr inż. arch. Arkadiusz Zientala uprawnienia budowlane nr 21/99 do projektowania i kierowania robotami budowlanymi bez ograniczeń w specjalności architektonicznej SLOIA nr SL-0237 nr SLK/50/5281/08
BRANŻA INSTALACJI SANITARNYCH	<u>PROJEKTANT</u> mgr inż. Krzysztof Popiela uprawnienia nr SLK/2516/PWOS/09 w specjalności instalacji sanitarnych	mgr inż. Krzysztof Popiela uprawnienia budowlane do projektowania i kierowania robotami budowlanymi bez ograniczeń w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń ciepłych, wentylacyjnych, gazowych, wodociągowych i kanalizacyjnych nr ewid. SLK/2516/PWOS/09
BRANŻA INSTALACJI ELEKTRYCZNYCH	<u>PROJEKTANT</u> mgr inż. Marcin Tront uprawnienia nr SLK/3640/PWOE/11 w specjalności instalacji elektrycznych	mgr inż. Marcin Tront Uprawnienia budowlane Nr SLK/3640/PWOE/11 do projektowania i kierowania robotami budowlanymi w spec. instalacyjnej w zakresie sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych bez ograniczeń
BRANŻA INSTALACJI ELEKTRYCZNYCH	<u>PROJEKTANT-sprawdzający</u> inż. Krystian Tront uprawnienia nr 189/98 w specjalności instalacji elektrycznych	inż. KRYSZTOF TRONT Uprawnienia budowlane do projektowania bez ograniczeń w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych, nr ewid. 189/98

nr arch: 001/2022

EGZ. 1

Jastrzębie-Zdrój, 19 styczeń 2022

SPIS TREŚCI

- Wytyczne Wojewódzkiego Urzędu Ochrony Zabytków w Opolu (str.4)

TOM I - BRANŻA ARCHITEKTONICZNA (str.5-6)

- Opis techniczny
- Część rysunkowa

A-01 RZUT 1 PIĘTRA - POM. SERWEROWNI - BRANŻA BUDOWLANA

TOM II - BRANŻA SANITARNA (str.7-8)

- Opis techniczny
- Część rysunkowa

K-01 PLAN INSTALACJI KLIMATYZACJI - RZUT 1 PIĘTRA

K-02 PLAN INSTALACJI KLIMATYZACJI - RZUT 2 PIĘTRA

K-03 PLAN INSTALACJI KLIMATYZACJI - RZUT PODDASZA

TOM III - BRANŻA ELEKTRYCZNA (str.9-18) **BRANŻA TELETECHNICZNA (str.19-115)**

- Opis techniczny
- Część rysunkowa

E-01/1 Plan instalacji elektrycznej – rzut piwnic

E-01/2 Plan instalacji elektrycznej – rzut parteru

E-01/3 Plan instalacji elektrycznej – rzut 1 piętra

E-01/4 Plan instalacji elektrycznej – rzut 2 piętra

E-01/5 Plan instalacji elektrycznej – rzut poddasza

E-02 Schemat ideowy zasilania w energię elektryczną

E-03 Schemat ideowy rozdzielnic TB-WLZ

E-04 Schemat ideowy rozdzielnic TB-GTK

E-05/1 – 05/4 Schemat ideowy rozdzielnic piętrowych komputerowych TB-K/...

E-06/1 – 06/4 Schemat ideowy rozdzielnic piętrowych bezpiecznikowych TB-K/...

T-01/2 Plan instalacji teletechnicznej (LAN, KD i CCTV) – rzut parteru

T-01/3 Plan instalacji teletechnicznej (LAN, KD i CCTV) – rzut 1 piętra

T-01/4 Plan instalacji teletechnicznej (LAN, KD i CCTV) – rzut 2 piętra

T-01/5 Plan instalacji teletechnicznej (LAN, KD i CCTV) – rzut poddasza

T-01/6 Plan instalacji teletechnicznej (SSP i SSNiW) – rzut piwnic

T-01/7 Plan instalacji teletechnicznej (SSP i SSNiW) – rzut parteru

T-01/8 Plan instalacji teletechnicznej (SSP i SSNiW) – rzut 1 piętra

T-01/9 Plan instalacji teletechnicznej (SSP i SSNiW) – rzut 2 piętra

- T-01/10 Plan instalacji teletechnicznej (SSP i SSNiW) – rzut poddasza
- T-02 Schemat ideowy okablowania strukturalnego
- T-03 Widok szafy GPD
- T-04 Schemat ideowy instalacji CCTV
- T-05 Schemat ideowy instalacji kontroli dostępu
- T-06 Schemat ideowy przejścia jednostronnego kontroli dostępu
- T-07 Schemat ideowy instalacji SAP
- T-08 Schemat ideowy instalacji SSNiW

Uprawnienia projektowe i oświadczenie projektantów

TOM I – Branża architektoniczna.

OPIS TECHNICZNY

• **Podstawa opracowania:**

- Dokumentacja archiwalna dostarczona przez Zamawiającego
- Wizja lokalna na obiekcie
- Dokumentacja zdjęciowa
- Warunki techniczne jakim powinny odpowiadać budynki i ich usytuowanie
- Protokół z okresowej kontroli technicznej obiektu budowlanego z 27.03.2018r

• **Zakres opracowania:**

- Fragment poziomu I piętra – istniejące pomieszczenie serwerowni w budynku ratusza miejskiego w Paczkowie

• **Stan istniejący pomieszczenia:**

- Na podstawie zapisów z kontroli obiektu - Strop pod serwerownią bez widocznych ugięć i pęknięć, brak klawiszowania stropu. Prawdopodobnie strop w konstrukcji drewnianej, belkowej.
- Posadzka drewniana z desek podłogowych, malowana farbami olejnymi
- Ściany zewnętrzne murowane i tynkowane tynkiem cementowo-wapiennym
- Ściany wewnętrzne murowane gr około 12 cm tynkowane tynkiem cementowo-wapiennym, częściowo ściany z płyt kartonowo-gipsowych
- Drzwi do pomieszczenia płytowe drewniane dwuskrzydłowe o szerokości skrzydła około 80,0 cm
- Sufit tynkowany tynkiem cementowo-wapiennym (dolna powierzchnia stropu)
- Instalacja elektryczna i teletechniczna
- Wentylacja pomieszczenia

• **Planowane roboty budowlane:**

- Rozbiórka kraty stalowej prowadzącej do wydzielonego pomieszczenia
- Budowa nowej ścianki działowej wydzielającej pomieszczenie serwerowni. Ścianak z płyt kartonowo-gipsowych na ruszcie stalowym (pełen system). Ścianka gr min 100 mm, o odporności gipsowej REI120
- Montaż nowych drzwi stalowych o odporności ogniowej EI60 z kontrolą dostępu i samozamykaczem
- Obłożenie pozostałych ścian wydzielonego pomieszczenia płytami kartonowo-gipsowymi na ruszcie stalowym bądź na packach klejowych, tak aby uzyskać odporność ogniową całej ściany REI120.
- Całą podłogę wydzielonego pomieszczenia należy wyłożyć wykładziną antystatyczną (cały system montażowy z cokolikami listwami, zamkami itp.). Przed ułożeniem wykładziny oczyścić istniejącą podłogę i ewentualnie uzupełnić lub naprawić istniejące deski podłogowe. Całość zabezpieczyć impregnatami do NRO

• **Nośność stropu:**

Planowane roboty związane z wydzieleniem pomieszczenia pod nową serwerownię nie spowodują zmiany obciążeń. Brak konieczności wzmacniania stropu.

• **Zestawie materiałów:**

- drzwi metalowe pełne z samozamykaczem EI60 930/2000 w klasie RC4 – 1 szt
- ścianka działowa (2x płyta G-K z wypełnieniem i ruszt stalowy) - około 5,60 m2
- okładzina pozostałej części ścian z płyt G-K o odporności ogniowej – 15,70 m2
- emulsja gruntująca do malowania ścian
- farba akrylowa do malowania ścian
- farba akrylowa do malowania sufitu
- istniejąca podłoga do oczyszczenia i impregnacji – około 5,10 m2
- nowa wykładzina antystatyczna na podłogę – około 5,10 m2

OPRACOWAŁ

mgr inż. arch. Arkadiusz Zientala
uprawnienia budowlane nr 24/99
do projektowania i kierowania robotami budowlanymi
bez ograniczeń w specjalności architektonicznej
SLOIA nr SL-0237 nr SLK/SLO/5281/08

TOM II – Branża Sanitarna.**OPIS TECHNICZNY**

Przedmiotem opracowania jest projekt instalacji klimatyzacji dla modernizowanego pomieszczenia serwerowni znajdującego się na pierwszym parterze Urzędu Miejskiego w Paczkowie przy ul. Rynek 1. Roboty, których dotyczy opracowanie obejmują czynności mające na celu wykonanie instalacji klimatyzacji w remontowanym pomieszczeniu serwerowni Urzędu Miasta w Paczkowie.

Zapotrzebowanie chłodu dla remontowanego pomieszczenia serwerowni:

Pomieszczenie serwerowni	- 0,8 kW.
Moc cieplna projektowanych urządzeń	- 4,0 kW.
Łączne zapotrzebowanie na chłód	- 4,8 kW

Zaprojektowano układ klimatyzacji o mocy nominalnej 5,20 kW w zakresie chłodzenia.

Zakres rzeczowy projektowanej instalacji obejmuje:

- montaż nowych urządzeń klimatyzacyjnych, jednostki wewnętrznej typu split na ścianie w remontowanym pomieszczeniu serwerowni, zaś jednostkę zewnętrzną należy zabudować na nieużytkowym poddaszu które ma zapewnioną niezbędną wentylację. Jednostkę zewnętrzną należy przytwierdzić do podłogi poddasza.
- montażu przewodów pomiędzy jednostką zewnętrzną i wewnętrzną ciecz gaz
- oraz montażu instalacji odprowadzającej skropliny za pomocą przewodu PP o średnicy 16 mm połączonego z pompką skroplin o wysokości podnoszenia min 15 m, przewód odprowadzający skropliny należy wpuścić do rynny na poddaszu.

Klimatyzację pomieszczenia projektuje się jako układu z jednostką typu split zabudowaną na ścianie wewnętrznej pomieszczenia połączoną z jednostką zewnętrzną zabudowaną na poddaszu nieużytkowym. Jednostkę klimatyzacyjną sterowana będzie pilotem lub aplikacją na smartfona. Pilot jaki aplikacja umożliwi wybór pracy, regulację temperatury, prędkości obrotowej wentylatora / kierunek nawiewu.

W poniższej tabeli przedstawiono charakterystyczne parametry projektowanego układu klimatyzacji

Parametry jednostki wewnętrznej	
Nominalna wydajność chłodnicza	5,20 kW
Nominalna wydajność grzewcza	5,30 kW

Klasa efektywności chłodzenie	A++
Klasa efektywności grzanie	A+
Wymiary Wys. x Szer. x Głęb. [mm]	300x224x970
Ciężar	13,5 kg
Poziom mocy akustycznej Chłodzenie	55-41 dBA
Zasilanie - Faza/Częstotliwość/Napięcie Hz/V	1~/50/220-240

Parametry jednostki Zewnętrznej	
Wymiary Wys. x Szer. x Głęb. [mm]	700x963x396
Ciężar	45 kg
Poziom mocy akustycznej chłodzenie	64 dBA
Zakres pracy Chłodzenie Temp. otoczenia Min.~Maks. °C	-15~43
Czynnik chłodniczy Typ/GWP	R-32/675
Zasilanie Faza/Częstotliwość/Napięcie	1~/50/220-240
Prąd – znamionowy chłodzenie	10,9 A

Jednostkę zewnętrzną należy usytuować podłódze pomieszczenia nieużytkowego strychu..

Odprowadzenie skroplin z urządzenia wykonać przy użyciu pompki skroplin przystosowanej do pracy z jednostkami o mocy do 10 kW. Odprowadzenie skroplin wykonać przewodem PP o średnicy Ø16 i włączyć do rynny na dachu obiektu. Połączenie pomiędzy jednostką zewnętrzną i wewnętrzną wykonać przewodami miedzianymi średnicy Ø 6.35/12.7 izolowanymi izolacją grubości min 9 mm. Izolacja powinna zawierać zewnętrzną warstwę ochronną. Przewody instalacyjne należy prowadzić w korycie instalacyjnym koloru białego. Połączenia elektryczne pomiędzy urządzeniami jaki zasilanie wykonać zgodnie w wytycznymi producenta układu klimatyzacji. Należy zabudować układ klimatyzacyjny z minimum dwuletnim okresem gwarancji.

OPRACOWAŁ

mgr inż. Krzysztof Popielec
uprawnienia budowlane do projektowania i kierowania
robotami budowlanymi bez ograniczeń, specjalność
instalacyjnej w zakresie sieci, instalacji i urządzeń ciepłych,
wentylacyjnych, gazowych, wodociągowych i kanalizacyjnych
dla budowl. 33.2.7216/7400/09



TOM III – Branża elektryczna i teletechniczna.

INSTALACJE ELEKTRYCZNE

PODSTAWA OPRACOWANIA

- Zlecenie Inwestora
- Obowiązujące normy i przepisy w zakresie opracowania.
- Architektoniczne podkłady budowlane
- Inwentaryzacja własna na obiekcie
- ustalenia na spotkaniu z Inwestorem
- wytyczne Wojewódzkiego Urzędu Ochrony Zabytków w Opolu
- Karty katalogowe wyrobów
- Dokumentacja zdjęciowa.

PRZEDMIOT OPRACOWANIA

Przedmiotem opracowania jest projekt instalacji elektrycznej i teletechnicznej dla modernizacji serwerowni wraz z instalacją strukturalną, dedykowaną instalacją elektryczną wewnątrz budynku Urzędu Miejskiego w Paczkowie.

Niniejsze opracowanie obejmuje następujące sieci i instalacje w budynku:

- sieci dedykowanej zasilania komputerów,
- gniazd wtyczkowych,
- wyłącznika PPOŻ,
- siłową,
- wewnętrzną instalację zasilania i rozdziału energii,
- przeciwporażeniową i wyrównania potencjałów
- przeciwprzepięciową,
- wewnętrzną sieć strukturalną (LAN) i telefoniczną,
- kontroli dostępu (KD),
- alarmową sygnalizacji pożaru (SAP),
- monitoringu wewnętrznego (CCTV),
- sygnalizacji napadu i włamania (SSNiW),
- odgromowa.

UWAGA!

- **Przyłącza energetyczne i teletechniczne istnieją, a modernizacja sieci nie wymaga zwiększenia mocy przyłączeniowej dla budynku.**

DANE ENERGETYCZNE

Napięcie zasilania : 400/230V ; 50Hz AC

Moc maksymalna:	$P_m=40\text{kW}$
Moc zainstalowana:	$P_i=72,7\text{ kW}$ (projektowana)
współczynnik jedn:	$k_j=0,55$
Pomiary energii:	istniejący (3 liczniki 3-fazowe, układ bezpośredni)
Układ sieci:	TNC-S
System ochrony:	szybkie wyłączenie oraz wyłączniki RCD

ZASILANIE W ENERGIĘ ELEKTRYCZNĄ

Istniejący budynek Urzędu Miasta zasilany jest istniejącym kablem YAKY 4x70 z złącza kablowego (nr 800176) na elewacji budynku. W zakresie modernizacji zasilania w związku z koniecznością zastosowania „przeciwpowozarowego wyłącznika prądu” należy:

- zabudować nowe złącze kablowe „przeciwpowozarowego wyłącznika prądu” ZK-W_POŻ pod tynkiem, z licowane z istniejącym złączem (nr 800176),
- za układem pomiarowym istniejący kabel zasilający oświetlenie zewnętrzne i fontannę pozostaje bez zmian,
- za układem pomiarowym dla TB-WIEŻA istniejący WLZ pozostaje, lecz należy w przedsiönku wieży zabudować **PWP-W** „przeciwpowozarowego wyłącznika prądu” dla wyłączenia obwodów elektrycznych zasilanych z TB-WIEŻA – przycisk musi być zasilany przewodem niepalnym PH90 jako zdublowanie-rozszerzenie „przeciwpowozarowego wyłącznika prądu” **PWP** dla budynku Urzędu Miasta.,
- od tablicy pomiarowej do ZK-W_POŻ ułożyć projektowane kable 2*(5*LGY35) jako zasilanie dla TB-WLZ i TB-W (wieża)
- od złącza ZK-W_POŻ ułożyć nowoprojektowany kabel YKYżo 5x35 dla zasilania tablicy TB-WLZ budynku Urzędu Miasta, istniejący kabel zasilający tablicę bezpiecznikową w wieży pozostaje bez zmian, należy go wprowadzić (mufując) do projektowanego ZK-W_POŻ.

POMIAR ENERGII ELEKTRYCZNEJ

Dla rozliczeń z Zakładem Energetycznym pomiar energii elektrycznej odbywać się zgodnie z stanem istniejącym. Istniejące trzy liczniki :

- (budynek wieży),
- (budynek Urzędu Miasta)
- (oświetlenie zewnętrzne z zasilaniem fontanny)

Wykonawca przed przystąpieniem do prac i rozplombowanie istniejących układów pomiarowych zobowiązany jest powiadomić służby techniczne Tauron Dystrybucja o planowanych pracach i uzyskać dopuszczenie do prac na sieci w związku z modernizacją obwodów i wyposażenie budynku w WYŁACZNIK POŻAROWY.

ROZDZIAŁ ENERGII – TABLICA TB-WLZ

Dla zasilania tablic bezpiecznikowych piętowych w budynku Urzędu Miasta istnieje tablica główna TB-WLZ na parterze w zabudowie wnekowej, którą należy zdemontować i w jej miejsce zabudować nową p.t.. Tablicę należy zastosować o stopniu ochrony IP30, zamykaną na klucz i wyposażyć w rozłączniki bezpiecznikowe jako zabezpieczenie obwodów zgodnie z rysunkiem E-03. Obudowę tablicy połączyć galwanicznie z szyną PE i główną szyną wyrównawczą GSW w pom. 0.7.

TABLICA TB-GTK

Dla zasilania tablic komputerowych w budynku Urzędu Miasta zaprojektowano tablicę główną komputerową TB-GTK. Dla zasilania głównej rozdzielni komputerowej „TB-GTK” przyjęto kabel YKYżo 5x16 na całej długości ułożony pod tynkiem. Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym bez domieszek cementu oraz pomalować w kolorystyce analogicznie do istniejącej.

TABLICE BEZPIECZNIKOWE TB-...

Dla zasilania wszystkich urządzeń gniazda 230V pod kserokopiarkę, tablicę SSNiW, kontroli dostępu, istniejące obwody oświetlenia podstawowego i ewakuacyjnego należy istniejące tablice bezpiecznikowe zdemontować a w ich miejsce zabudować nowe TB (piętrowe) w zabudowie natynkowej, IP30. Tablice zasilic z nowoprojektowanego pola odpływowego (proj. rozłącznik bezpiecznikowy) z projektowanej TB-WLZ. Przewód zasilający układać analogicznie z innymi przewodami – kablami elektroenergetycznymi tj. pod tynkiem. Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym bez domieszek cementu oraz pomalować w kolorystyce analogicznie do istniejącej.

PRZECIWPOŻAROWY WYŁĄCZNIK PRĄDU

Przyciski **PWP** i **PWP-W** przeciwpożarowego wyłącznika prądu należy zainstalować przy wyjściu głównym z budynku urzędu miasta i wieży. Naciśnięcie któregokolwiek przycisku **PWP** powoduje zadziałanie cewki wybijakowej wyłącznika pożarowego w ZK-W_POŻ i w konsekwencji całego budynku włącznie z wieżą. Przyciski **PWP** zabudować w obudowie koloru czerwonego z szybką oraz oznaczyć zgodnie z PN. Z projektowanego złącza ZK-W_POŻ do projektowanych przycisków przeciwpożarowych **PWP** i **PWP-W** należy wyprowadzić przewód HDGs 3x2,5 PH90. Jako główny wyłącznik pożarowy zastosować rozłączniki mocy LN-1 160A z cewką wzrostową. Cewkę wyłącznika W-POŻ zabezpieczyć zabezpieczeniem CLS6 C6A/3. Zastosować cewkę wzrostową. Przewody prowadzić pod tynkiem. **Nad przyciskami PWP przykleić oznaczenie „Przeciwpożarowy Wyłącznik Prądu”**

WYŁĄCZNIK GŁÓWNY KOTŁOWNI

Wyłącznik kotłowni WGK należy zainstalować przy zejściu do piwnicy. Wyłącznik wyposażyc w rozłącznik główny (izolacyjny) IS-100/3 100A. Rozłączenie rozłącznika **WGK** spowoduje odłączenie tablicy-obwodów kotłowni od zasilania. Przewody prowadzić pod tynkiem. Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym bez domieszek cementu oraz pomalować w kolorystyce analogicznie do istniejącej. Umieszczenie **WGK** przedstawiono na rys. E-01_2.

INSTALACJA SIŁOWA

W skład instalacji siłowej wchodzi zasilanie:

- klimatyzatorów,
- punktów szaf dystrybucyjnych,
- centralę kontroli dostępu,
- centralę SSWiN.

Z rozdzielnic komputerowych TB-K/.. oraz RK-SE, wyprowadzić przewody do gniazd [PEL] i szafy rackowej w pom. serwerowni. Rozmieszczenie urządzeń siłowych oraz plan prowadzenia

instalacji przedstawiono na rys. kondygnacji. Przewody prowadzić pod tynkiem. Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym bez domieszek cementu oraz pomalować w kolorystyce analogicznie do istniejącej.

Centralę systemu kontroli dostępu, centralę SSWiN, klimatyzatory, zasilić bezpośrednio z wydzielonego obwodu z tablicy bezpiecznikowej TB-..... z pominięciem gniazda.

Klimatyzator uruchamiany za pomocą regulatora LCD.

Przy przejściu kabli przez zewnętrzne ściany pomieszczenia serwerowni zadławić masą ognioochronną EI-120.

INSTALACJA PRZECIWPORAŻENIOWA

PODSTAWOWA OCHRONA PRZED PORAŻENIEM PRĄDEM ELEKTRYCZNYM

Podstawowa ochrona przed rażeniem prądem (ochrona przed dotykiem bezpośrednim) jest zapewniona przez izolowanie części czynnych.

W instalacji zaprojektowano również wyłączniki ochronne różnicowoprądowe, które w przypadku jakiegokolwiek pogorszenia się stanu izolacji w instalacji i przekroczeniu prądu zadziałania wyłącznika, powodują wyłączenie kontrolowanego odcinka instalacji elektrycznej. Dla zakresu opracowania dobrano wyłączniki różnicowoprądowe RCD o prądzie zadziałania 30mA. Przez zastosowanie wyłączników ochronnych osiągnięto dodatkowe zabezpieczenie przed przypadkowym bezpośrednim dotknięciem (nieuziemionego) elementu znajdującego się pod napięciem.

DODATKOWA OCHRONA PRZED PORAŻENIEM PRĄDEM ELEKTRYCZNYM

Jako dodatkową ochronę przed porażeniem prądem elektrycznym przewidziano w niniejszym obiekcie - szybkie wyłączenie: układ sieciowy TNC-S. Instalację 1-fazową należy wykonać jako 3-przewodową /L+N+PE/, a 3-fazową jako 5-przewodową /L1,L2,L3,N,PE/. Miejsce rozdziału przewodu ochronno- neutralnego PEN na przewód ochronny PE i neutralny istnieje w złączu ZK przy budynku. Sprawdzić rezystancję uziemienia, która nie powinna przekroczyć wartości 10 Ω .

Obudowy metalowe całego osprzętu elektrycznego, obudowy tablic rozdzielczych należy przyłączyć do przewodu ochronnego (PE).

Połączeniami wyrównawczymi, o których mowa w ust. 1 pkt 7 Rozporządzenia Ministra Infrastruktury z dnia 12 marca 2009, należy objąć:

- metalowe elementy przewodów i urządzeń do wentylacji i klimatyzacji,
- metalowe elementy obudowy urządzeń instalacji telekomunikacyjnej.

Od projektowanego złącza ZK-W_POŻ w budynku przewodem ochronnym jest przewód PE. Obudowy metalowe całego osprzętu elektrycznego użytego w instalacji należy przyłączyć do przewodu ochronnego (PE).

INSTALACJA PRZECIWPRIEPĘCIOWA

Dla ochrony przed przepięciami w projektowanym złączu ZK-W_POŻ zabudowano ograniczniki przepięć I stopnia, a w istniejących i projektowanych tablicach bezpiecznikowych projektuje się ograniczniki przepięć II stopnia.

Zastosowane zabezpieczenia ograniczają przepięcia w sieci do wartości 1÷1,5kV. Są to wartości napięć jakie wytrzyma większość urządzeń elektrycznych i elektronicznych.

INSTALACJE OŚWIETLENIA PODSTAWOWEGO i AWARYJNEGO EWAKUACYJNEGO

Istniejące obwody oświetlenia podstawowego, nocnego oraz awaryjnego-ewakuacyjnego należy wpiąć w nowoprojektowane tablice bezpiecznikowe piętrowe.

INSTALACJA GNIAZD WTYCZKOWYCH

Instalację gniazd wtyczkowych podtynkowych wykonać analogicznie do instalacji teletechnicznej gniazd (LAN + TEL). Przewody należy układać pod tynkiem. Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym bez domieszek cementu oraz pomalować w kolorystyce analogicznie do istniejącej. Zastosować przewody YDYżo 3x2,5 450/750V.

Wysokość umieszczenia gniazd:

- gniazda w pomieszczeniach biurowych – 0,3 m nad podłogą
- gniazda w WC i pom. technicznych - 1,35 m nad podłogą
- gniazda w zestawach z zasilaniem dedykowanym jako systemowe we wspólnej ramce w standardzie 45x45mm – 0,3m nad podłogą

Zastosować gniazda podwójne z uziemieniem, a w pomieszczeniach wilgotnych pojedyncze z uziemieniem i z klapką o stopniu szczelności IP 44, a w zestawach gniazda pojedyncze modułowe 45x45. Na zestaw gniazd skład się;

- 2x gniazdo DATA,
- 1x gniazdo zwykłe 230V,
- 3x gniazdo sieci strukturalnej RJ45 kat.6,

Kolorystykę gniazd ogólnych dobrać do wystroju wnętrza, a system dopasować do gniazd sieci teletechnicznych.

Trasę przewodów elektrycznych układać oddzielnie od instalacji teletechnicznych.

INSTALACJA SIECI DEDYKOWANEJ ZASILANIA KOMPUTERÓW

Zasilanie stanowisk komputerowych w pomieszczeniach biurowych odbywać się będzie z tablic komputerowych TB-K/... Poszczególne obwody zasilania komputerów zabezpieczono wyłącznikami różnicowo-prądowymi o charakterystyce A.

Gniazda zasilające dedykowane wykonane są w standardzie **DATA** koloru czerwonego z kluczem, uniemożliwiającym podłączenie innych urządzeń poza komputerowymi (stacja robocza, monitor). Gniazda pojedyncze modułowe we wspólnej ramce.

Zasilanie dedykowane należy wykonać przewodami YDYżo 3x2,5 prowadzonymi analogicznie do instalacji gniazd ogólnych 230V tj. pod tynkiem. Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym bez domieszek cementu oraz pomalować w kolorystyce analogicznie do istniejącej

INSTALACJA ODGROMOWA

1. Podstawy normatywne

Norma PN EN 62305 składa się z następujących części:

- PN EN 62305-1:2008 - „Ochrona odgromowa – Część 1: Zasady ogólne“

- PN EN 62305-2:2008 - „Ochrona odgromowa – Część 2: Zarządzanie ryzykiem“
- PN EN 62305-3:2009 - „Ochrona odgromowa – Część 3: Uszkodzenia fizyczne obiektów i zagrożenie życia“
- PN EN 62305-4:2009 - „Ochrona odgromowa – Część 4: Urządzenia elektryczne i elektroniczne w obiektach“

2. Ryzyko i źródło uszkodzeń

Aby uniknąć strat w przypadku trafienia pioruna w obiekt, przewiduje się zastosowanie specyficznych środków ochrony dla danego chronionego obiektu. W normie PN EN 62305-2:2008 opisana jest analiza ryzyka i środki ochrony odpowiednie do występującego zagrożenia w obiekcie. Celem analizy ryzyka jest, aby obliczone istniejące ryzyko ograniczyć do wartości akceptowanej (tolerowanej) RT przez dobór odpowiednich środków ochrony.

Bieżąca analiza ryzyka wg PN EN 62305-2:2008 dla projektu URZĄD GMINY PACZKÓW - obiekt Obiekt wskazuje na konieczność zastosowania środków ochrony. Wartość ryzyka dla obiektu została określona i, jeśli to konieczne, muszą być dobrane środki ochrony do redukcji ryzyka. Wynikiem analizy ryzyka jest nie tylko wybór klasy ochrony odgromowej (LPL I, II, III lub IV) lecz szereg środków ochrony włącznie ze środkami do redukcji pola magnetycznego, czyli ochrony przed LEMP.

W rezultacie należy dobrać uzasadnione ekonomicznie środki ochrony, odpowiednie do właściwości istniejącego budynku oraz jego aktualnego wykorzystania.

3. Informacje o projekcie

3.1 Wybór ryzyka do uwzględnienia

Ze względu na rodzaj i wykorzystanie obiektu Obiekt, zostały wybrane i uwzględnione następujące ryzyka:

Ryzyko R1: Ryzyko utraty życia ludzkiego; RT: 1,00E-05

Akceptowane wartości poszczególnych części ryzyka RT zostały określone. Wartości akceptowane ryzyka dla R1, R2, R3 oraz R4 zostały podane w normie.

Celem analizy ryzyka jest, aby istniejące ryzyko ograniczyć do wartości akceptowanej (ponoszonej) RT przez dobór odpowiednich środków ochrony uzasadnionych ekonomicznie, które to ryzyko ograniczą do akceptowanego poziomu.

Celem analizy ryzyka jest, aby istniejące ryzyko ograniczyć do wartości akceptowanej (ponoszonej) RT przez dobór odpowiednich środków ochrony uzasadnionych ekonomicznie, które to ryzyko ograniczą do akceptowanego poziomu.

3.2 Parametry geograficzne i budynku

Podstawą analizy ryzyka zgodnie z normą PN EN 62305-2:2008 jest gęstość piorunowych wyładowań doziemnych Ng. Określa ona liczbę bezpośrednich wyładowań piorunowych

doziemnych na km² na rok [1/rok/km²]. Wartość 3,10 wyładowań piorunowych na km² na rok została określona dla położenia obiektu Obiekt przy wykorzystaniu mapy gęstości piorunowych wyładowań doziemnych. W rezultacie ze względu na położenie obiektu liczba dni burzowych wynosi 31,00 rocznie.

Wymiary budynku decydują o zagrożeniu bezpośrednim uderzeniem pioruna. Powierzchnie zbierania bezpośrednich / pośrednich uderzeń pioruna są określone w oparciu o te wymiary. Obiekt Obiekt ma następujące wymiary:

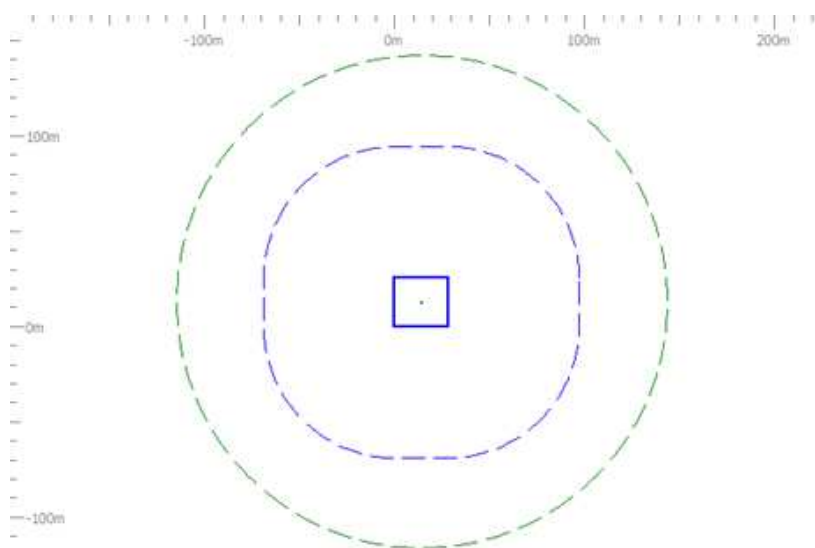
Lb	Długość:	29,00 m
Wb	Szerokość:	26,00 m
Hb	Wysokość:	23,00 m
Hp	Najwyższy punkt obiektu (jeśli występuje):	43,00 m

Uwzględniając wymiary obiektu, obliczono następujące powierzchnie zbierania:

Powierzchnia zbierania wyładowań bezpośrednich: 52 279,00 m²

Powierzchnia zbierania wyładowań pośrednich: 224 603,00 m

(obok obiektu)



Środowisko otaczające obiekt jest istotnym czynnikiem określającym liczbę możliwych bezpośrednich / pośrednich uderzeń pioruna. Dla obiektu Obiekt jest ono zdefiniowane następująco:

Względne położenie Cdb: 0,50

Jeśli gęstość piorunowych wyładowań doziemnych odnosi się do wielkości i środowiska obiektu, należy oczekiwać częstości:

- bezpośrednich uderzeń pioruna w obiekt: ND = 0,081 uderzeń / rok,

- pośrednich uderzeń w obiekt: $NM = 0,6152$ uderzeń / rok.

3.3 Podział obiektu na strefy / strefy ochrony odgromowej

Obiekt budowlany Obiekt nie został podzielony na strefy ochrony odgromowej/inne strefy.

3.4 Linie zasilające

Wszystkie linie wchodzące i wychodzące z budynku są uwzględniane w analizie ryzyka. Przewodzące rury nie są uwzględniane jeśli są podłączane do głównej szyny uziemiającej. Jeśli nie są uziemione to należy je uwzględnić w analizie ryzyka (wymagania wyrównania potencjałów!).

W analizie ryzyka dla budynku Obiekt uwzględniono następujące linie:

- KABEL WLZ

Dla każdej linii określono parametry, jak np.:

- Rodzaj linii (napowietrzna/podziemna)
- Długość linii (na zewnątrz budynku)
- Otoczenie
- Przyłączony obiekt do linii
- Typ wewnętrznego okablowania (ekranowane/nieekranowane)
- Najmniejsze napięcie wytrzymywane wyposażenia (wytrzymałość urządzeń odbiorczych).

W oparciu o to, ryzyko dla obiektu i jego zawartości z powodu trafienia pioruna w linię lub obok linii, zostało określone i uwzględnione w analizie ryzyka.

3.5 Ryzyko pożaru

Ryzyko pożaru w obiekcie stanowi ważnym czynnikiem determinującym wybór koniecznych środków ochrony. Ryzyko pożaru dla danego obiektu Obiekt określono następująco:

- Zwykłe

3.6 Środki podjęte w celu minimallizacji skutków pożaru

Zostały zaznaczone następujące środki ochrony służące do ograniczenia ryzyka pożaru:

- Stałe automatycznie działające instalacje gaszące, automatyczne instalacje alarmowe

3.7 Specjalne zagrożenia w budynku dla zdrowia i życia ludzkiego

Ze względu na liczbę osób, ryzyko paniki dla obiektu Obiekt ustalono na następującym poziomie:

- Niski poziom paniki (nie więcej niż 100 osób)

4. Analiza ryzyka

Jak opisano w 3.1, zostały przyjęte następujące ryzyka 5.

Niebieski pasek przedstawia wartość tolerowaną (akceptowaną) ryzyka określoną w normie, pasek **zielony** / **czerwony** przedstawia wartość bieżącą obliczanego ryzyka.

4.1 Ryzyko R1, Utrata życia ludzkiego

Dla osób na zewnątrz i wewnątrz budynku Obiekt ustalono następujące ryzyko:

Tolerowane Ryzyko RT:	1,00E-05
Obliczone Ryzyko R1 (brak ochrony):	2,27E+000
Obliczone Ryzyko R1 (bez ochrony):	4,54E-06



Aby zredukować istniejące ryzyko, stosuje się środki ochrony opisane w 4.

4.2 Wybór środków ochrony

Ryzyko zostało zredukowane do akceptowanego poziomu przez dobór następujących środków ochrony.

Ten dobór środków ochrony jest częścią zarządzania ryzykiem dla obiektu Obiekt i jest właściwy tylko w odniesieniu do tego obiektu.

Środki ochrony Z ochroną / stan docelowy:

Powierzchnia	Środki ochrony	Współczynnik
	Wewnętrzna charakterystyka gruntu / podłogi	
ru:	Asfalt, linoleum, drewno	1.000E-05
	$\geq 100 \text{ k}\Omega$	
	Ochrona przeciwpożarowa	
rp:	Stałe automatycznie działające instalacje gaszące, automatyczne instalacje alarmowe	2.000E-01

5. Obowiązek prawny

Dane o obiekcie, które przyjmuje się do obliczeń, powinny opierać się na informacji zarządzającego obiektem, właściciela lub właściwych służb lub też powinny być zebrane na miejscu. Zwraca się uwagę, że te dane muszą być jeszcze raz formalnie potwierdzone. Sposób postępowania przy dokonywaniu obliczeń ryzyka użyty w programie DEHNsupport odpowiada normie PN EN 62305-2:2008.

Zwraca się uwagę, że wszystkie założenia, materiały, odwzorowania, rysunki, wymiary, parametry oraz wyniki nie są prawnie wiążące dla osoby wykonującej analizę ryzyka.

ZGODNIE Z POWYŻSZYMI WYNIKAMI OBLICZEŃ

DLA OBIEKTU NIE JEST WYMAGANE WYKONANIE INSTALACJI OCHRONY ODGROMOWEJ

INSTALACJA LOKALNEGO UZIEMIENIA POSADZEK ANTYELEKTROSTATYCZNYCH.

W pomieszczeniu serwerowni będzie instalacja lokalnego uziemienia posadzek antyelektrostatycznych, do której należy przyłączyć wszystkie stałe metalowe przedmioty i urządzenia w tych pomieszczeniach jak : zaciski uziemiające, posadzki antyelektrostatyczne, grzejniki, ościeżnice drzwi, tablice, itp.

OCHRONA PRZED GROMADZENIEM ŁADUNKU ELEKTROSTATYCZNEGO

Na podłodze w pomieszczeniu serwerowni będzie wykonana przewodząca wylewka samopoziomująca przewodząca w której będzie np. zatopiony płaskownik Cu podłączony do szyny PE (w układzie TNC-S) w rozdzielnicy zasilającej GTK. Następnie należy ułożyć przewodzącą wykładzinę podłogową posiadającą atest w zakresie elektryczności statycznej.

UWAGI KOŃCOWE

1. Urządzenia objęte niniejszym projektem powinny być poddane kwalifikacji jakości i oznaczone znakiem bezpieczeństwa i dopuszczone do stosowania w budownictwie ze znakiem CE według dyrektyw Unii Europejskiej.
2. Całość instalacji wykonać zgodnie z „Warunkami technicznymi wykonania i odbioru robót montażowych – część V. Instalacje elektryczne” i zasadami wiedzy technicznej.
3. Wszystkie elementy metalowe instalacji elektrycznej, które nie posiadają fabrycznego zabezpieczenia przed korozją, należy pomalować farbą rdzochronną. Płaskowniki i druty stalowe ocynkowane należy sprawdzić na ciągłość ocynkowania.
4. Instalacje elektryczne wykonać należy po wykonaniu prac instalacyjnych i budowlanych. W trakcie robót budowlano-montażowych i posadzkarskich, należy skoordynować układanie rur ochronnych, wnęk, przepustów.
5. Po wykonaniu robót należy przeprowadzić odpowiednie próby i pomiary.
6. Projekt rozpatrywać łącznie z projektem architektonicznym, konstrukcyjno-budowlanym, instalacji wod-kan, c.o., wentylacji i klimatyzacji
7. Wszystkie roboty wykonać zgodnie z niniejszym projektem oraz obowiązującymi przepisami i normami.
8. Wszelkie zmiany w trakcie realizacji uzgodnić z projektantem z Opolskim Wojewódzkim Konserwatorem Zabytków i inspektorem nadzoru. W razie odstępstw od rozwiązań projektowych uzyskać akceptację autora projektu.
9. Przed oddaniem do eksploatacji należy dokonać pomiarów wielkości elektrycznych, a w szczególności pomiar stanu izolacji i pomiar rezystancji uziemienia.
10. W czasie prac montażowych miejsca niebezpieczne zabezpieczyć przed dostępem osób postronnych.
11. Przy przejściu przez zewnętrzne ściany budynku kable powadzić w rurach ochronnych i zadławić silikonem, pianką montażową, a w razie przejścia przez strefę pożarową zadławić masą ognioochronną EI-120.
12. Dopuszcza się zastosowanie produktów równoważnych o nie gorszych parametrach.

OPRACOWAŁ:

INSTALACJE TELETECHNICZNE

1 INSTALACJA SIECI STRUKTURALNEJ LAN

Podstawa opracowania projektu

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

Normy europejskie dotyczące ogólnych wymagań oraz specyficznych dla środowiska biurowego:

- PN-EN 50173-1:2018 Technika Informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne.
- PN-EN 50173-2:2018 Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Pomieszczenia biurowe.

Dodatkowe normy europejskie związane z planowaniem powołane w projekcie:

- PN-EN 50174-1:2018 Technika informatyczna. Instalacja okablowania – Część 1 – Specyfikacja instalacji i zapewnienie jakości.
- PN-EN 50174-2:2018 Technika informatyczna. Instalacja okablowania – Część 2 – Planowanie i wykonywanie instalacji wewnątrz budynków.
- PN-EN 50174-3:2014 Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków.
- ISO/IEC 14763-3:2014 Implementation and operation of customer premises cabling – Part 3: Testing of optical fibre cabling.
- PN-EN 50310:2016 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym.
- PN-EN 60794-1-1:2016-06 - Kable światłowodowe - Część 1-1: Wymagania wspólne - Postanowienia ogólne.
- IEEE P802.3bt-2018 Standard for Ethernet Amendment 2: Power over Ethernet over 4 Pairs.
- ISO/IEC 11801:2017 – Information technology – Generic cabling for customer premises specifies.

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

Uwaga: W przypadku powołań normatywnych niedatowanych obowiązuje najnowsze wydanie cytowanej normy.

1.2 Wymagania ogólne dotyczące okablowania strukturalnego

- Okablowanie strukturalne budowane jest zgodnie z w/w normami, tj. w konfiguracji gwiazdy i przy rygorze, że łącza stałe nie mogą przekroczyć długości 90 m.
- Ilość i rozmieszczenie gniazd przyjęto na podstawie informacji podanych przez Użytkownika. W trakcie realizacji, ostateczna lokalizacja gniazd logicznych w pomieszczeniach (bez zmiany ich ilości) powinna być ustalona pomiędzy Użytkownikiem, a Wykonawcą.
- Okablowanie ma być doprowadzone do punktu dystrybucyjnego znajdującego się w pomieszczeniu serwerowni na 1 Piętrze budynku, lokalizacja zgodnie z rzutami budowlanymi;
- Osłona zewnętrzna kabla w okablowaniu poziomym oraz szkieletowym ma być trudnopalna i niewydzielająca trujących substancji w obecności ognia;
- Okablowanie strukturalne w budynku obsługiwane jest przez Główny Punkt Dystrybucyjny GPD w pomieszczeniu serwerowni;
- Okablowanie poziome ma być prowadzone podwójnie ekranowanym kablem typu S/FTP kat. 7 w powłoce zewnętrznej LSFRZH;
- Wszystkie elementy pasywne składające się na okablowanie strukturalne muszą być oznaczone nazwą lub znakiem firmowym, tego samego producenta okablowania i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu 25-letniej gwarancji udzielonej bezpośrednio przez w/w producenta;
- Należy zastosować renomowany i sprawdzony w wielu instalacjach, nie tylko w Polsce, ale i w innych krajach Unii Europejskiej, system okablowania strukturalnego. Należy zastosować przetestowany system, którego producent ma, co najmniej 15-letnie doświadczenie w produkcji okablowania strukturalnego. Zakres jego działalności w całym tym okresie musi obejmować produkcję okablowania miedzianego (kable skrętkowych, złączy RJ45);
- Aby zagwarantować Użytkownikowi najwyższą jakość w zakresie projektowanego rozwiązania i komponentów, producent oferowanego systemu okablowania strukturalnego (miedzianego) musi spełniać najwyższe wymagania jakościowe potwierdzone następującymi programami i certyfikatami Six Sigma (status Belt), Premium Verification Program (PVP GHMT) oraz ISO 9001;
- Certyfikaty wydane przez międzynarodowe, renomowane niezależne laboratoria badawcze potwierdzające zgodność okablowania miedzianego z najnowszymi, aktualnymi normami okablowania strukturalnego ISO/IEC 11801 lub EN 50173;

- Wszystkie produkty muszą być fabrycznie nowe;
- Montaż gniazd okablowania poziomego PEL ma być realizowana podtynkowo przy zastosowaniu płyt czołowych prostych lub skośnych z uchwytami w standardzie 45x45, w zależności od typu instalowanego modułu;
- Wszystkie kable okablowania poziomego mają być zakończone w osprzęcie połączeniowym zgodnie z normą PN-EN 50173-1.
- Okablowanie poziome ma być zbudowane w oparciu o kabel ekranowany S/FTP kat. 7, powłoka zewnętrzna LSFRZH Dca;
- Do każdego punktu logicznego PEL należy doprowadzić jeden lub trzy kable ekranowane S/FTP kat. 7, przy czym punkty PL pojedyncze dedykowane są do obsługi systemów bezpieczeństwa CCTV, KD, SSP, SSWIN, natomiast punkty potrójne PEL dedykowane są obsłudze sieci LAN;
- PEL składa się z jednego gniazda systemu otwartego oraz dwóch gniazd systemu modularnego;

System z wymiennymi gniazdami (otwarty):

- Do każdego punktu logicznego PEL należy doprowadzić jeden kabel ekranowany S/FTP kat. 7, powłoka zewnętrzna LSFRZH Dca i zakończyć w osprzęcie połączeniowym w puszcze podtynkowej;
- W momencie instalacji należy zapewnić w punktach logicznych:
 - § Dostęp do gniazd 1xRJ45 kategorii 6_A systemu otwartego + 2xRJ45 kategorii 6_A systemu modularnego;
- Wszystkie łącza okablowania poziomego systemu otwartego mają zapewniać:
 - § Możliwości transmisyjne do minimum klasy E_A, co ma być potwierdzone certyfikatem pomiarowym wydanym na kanał lub łącze przez akredytowane niezależne laboratorium (np. Delta, GHMT) oraz powykonawczo pomiarami wykonanymi na obiekcie z gniazdem kat.6A.
 - § Możliwość zmiany typu gniazda na inny znajdujący się w normach ISO/IEC 11801 EN50173-1: RJ45, ARJ45, TERA złącze E_A.
 - § Możliwość zmiany kategorii gniazd na kat. 5, kat.6, kat.7 i kat.7_A.
 - § Możliwość współdzielenia jednego kabla dla kilku aplikacji w następujących konfiguracjach:
- 2 x Fast Ethernet z wykorzystaniem gniazd RJ45 kat.5, kat.6, kat.6_A,
- 2 x ISDN z wykorzystaniem gniazd RJ45 kat.5, kat.6, kat.6_A,

- Fast Ethernet + ISDN z wykorzystaniem gniazd RJ45 kat.5, kat.6, kat.6A,
- Gigabit Ethernet + ISDN z wykorzystaniem gniazd RJ45,
- 2 x telefon analogowy + Fast Ethernet z wykorzystaniem gniazd RJ45,
- 4 x telefon analogowy z wykorzystaniem gniazd RJ45 kat.3,
- 1 x telefon analogowy + 1x Fast Ethernet + 1x CATV z wykorzystaniem gniazd RJ45 i złącza F,
- 1x TERA o wydajności Kat.7A
- 1 x ARJ45 o wydajności Kat.7A

§ System ma zapewniać możliwość wielokrotnej zmiany typu gniazda, jego kategorii oraz współdzielenia kabla dla wielu aplikacji przy czym czynności te mają być wykonywane samodzielnie przez Użytkownika bez ingerowania w rozszycie kabla na osprzęcie połączeniowym bez potrzeby ponownego zarabiania gniazd, ponownego wykonywania pomiarów oraz instalowania dodatkowych elementów w postaci paneli krosowych i płyt czołowych w punktach logicznych.

§ Nie dopuszcza się stosowania gniazd i wtyków z niestandardowymi interfejsami (takimi, do których nie ma referencji w dokumentach z Rozdziału 2).

- Okablowanie poziome systemu otwartego należy zakończyć w punkcie dystrybucyjnym w panelach krosowych. Należy zastosować panele krosowe proste o wysokości 2U, niezaladowane na 24 oddzielne moduły gniazd ekranowanych;

System z modułami RJ45 (modularny):

- Okablowanie ma być realizowane poprzez ekranowane moduły gniazd RJ45 kat. 6A składające się z dwóch elementów, posiadających zacisk ekranu kabla (360o);
- Budowa wewnętrzna modułu gniazda RJ45 musi zapewniać:
- Zachowanie poprawnych parametrów transmisyjnych przy łączach stałych wynoszących 7m lub krótszych oraz kanałach wynoszących 11m lub krótszych;
- Zachowanie poprawnych parametrów transmisyjnych przy krótkich kanałach składającym się z wielu gniazd w bliskim sąsiedztwie. Dopuszcza się komponenty dzięki którym można zbudować kanały transmisyjne o długości 17m lub krótszych złożone z 4 gniazd;
- Należy zastosować modułowe panele krosowe kątowe o wysokości 1U, niezaladowane, które mają zapewnić zamontowanie 24 modułów z możliwością wprowadzenia, co najmniej 24 kabli

- Moduł gniazda ze stałym interfejsem RJ45 kat. 6_A należy zamontować w skośnej płycie czołowej 45x22,5 – uchwyt typu M45.
- System okablowania strukturalnego powinien zapewniać pełne wsparcie dla standardów PoE i zgodność z wymaganiami IEEE 802.3af i IEEE 802.3at, IEEE 802.3bt (typ 3 i 4) dla aplikacji PoE, PoE+, PoE++ 802.3af (PoE+) przy zachowaniu żywotności gniazd wynoszącym minimum 750 cykli połączeniowych (tj. utrzymaniu wymaganych minimalnych parametrów elektrycznych i transmisyjnych);
- Moduły gniazda muszą być w pełni zgodne z wymaganiami metod badawczych określonych w normach IEC 60512-99-01 i IEC 60512-99-002 w celu zapewnienia, że w przypadku wystąpienia łuku elektrycznego nie uszkodzi to krytycznego punktu styku wtyku i gniazda, co musi być potwierdzone przez testy wykonane przez producenta;
- Wszystkie miedziane kable krosowe muszą pochodzić od tego samego producenta co reszta komponentów okablowania strukturalnego.
- Środowisko wewnątrz budynku, w którym będzie instalowany osprzęt kablowy, jest środowiskiem biurowym i zostało ono sklasyfikowane, jako M₁I₁C₁E₂ zgodnie z normą PN-EN 50173-1; maksymalne długości kanałów transmisyjnych okablowania poziomego zostały obliczone dla najgorszego przypadku wzrostu temperatury otoczenia, tj. do 40°C.

1.3 Prowadzenie okablowania poziomego

Ze względu na to iż budynek Ratusza podlega ochronie konserwatorskiej trasy okablowania należy wykonać zgodnie z zaleceniami Opolskiego Wojewódzkiego Konserwatora Zabytków, a także w sposób, który ma zapewniać łatwe, bezkolizyjne i bezpieczne prowadzenie kabli uwzględniając inne instalacje w budynku. Okablowanie należy prowadzić w następujący sposób:

- Przewody instalacyjne prowadzić podtynkowo;
- Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym, bez domieszek cementu oraz pomalować w kolorystyce analogicznej do istniejącej;
- Wskazane jest prowadzenie tras kablowych w części przypodłogowej ścian;
- Nie dopuszcza się prowadzenia linii kablowych w obrębie zachowanych w budynku sklepień kolebkowych;
- W Sali obrad ochronie podlega bogata dekoracja sztukatorska na ścianach i sklepieniu oraz drewniane boazerie, w związku z powyższym linię kablową należy ułożyć tak, aby zapewnić maksymalną ochronę substancji zabytkowej wyżej wymienionych elementów zdobniczych;

· Separacja okablowania poziomego od kabli elektrycznych

Kable okablowania strukturalnego oraz elektrycznego, zgodnie z wymogami norm, należy prowadzić w oddzielnych trasach kablowych przy zachowaniu minimalnej separacji.

Należy przewidzieć odpowiednie zapasy miejsca w trasach kablowych stanowiące min. 20% pojemności tras kablowych dla całości okablowania.

· Prowadzenie okablowania w pionach kablowych

Trasy kablowe – pionowe należy wykonać podtynkowo a w pom. serwerowni w postaci drabinki kablowej pozwalającej na zamocowanie kabli oraz zachowanie odpowiednich promieni gięcia wiązek kablowych na zakrętach. W przypadku przebić/przejsć pomiędzy kondygnacjami należy zastosować zabezpieczenie zgodne z zasadami PPOŻ EI-120.

1.4 Okablowanie radiotelefonu

Okablowanie przeznaczone pod realizację łącza radiotelefonicznego należy poprowadzić w pomieszczenia 1.18 na parterze budynku do poziomu poddasza. W pomieszczeniu 1.18 oraz na poddaszu należy pozostawić odpowiedni zapas kabla, pozwalający na swobodne podłączenie linii radiotelefonu do urządzenia końcowego w pomieszczeniu 1.18 oraz podłączenia anteny radiotelefonu umieszczonej na dachu budynku ratusza.

Kabel przeznaczony do łącza radiotelefonicznego należy wykonać w oparciu o przewód koncentryczny zgodny ze specyfikacją projektową.

Tabela 1 Wymagania dla kabla koncentrycznego systemu radiotelefonicznego

Budowa kabla	Pleciony kabel koncentryczny
Pasma częstotliwości pracy	30 – 6000 MHz
Moc szczytowa	16kW
Skuteczność ekranowania	90 dB
Prędkość	85%
Impedancja kabla	50 omów
Pojemność	78 pF/m
Rezystancja prądu stałego, przewód wewnętrzny	4,69 omów/km

Rezystancja prądu stałego, przewód zewnętrzny	5,61 omów/km
Maksymalna częstotliwość	16,2 GHz
Średnica nad dielektrykiem	7.24 mm
Średnica nad płaszczem	10.29 mm
Średnica na taśmie	7.391 mm
Rozmiar nominalny	0.400 in
Materiał opłotu	Miedź cynowana
Pianka z materiału dielektrycznego	PE
Materiał płaszcza Niehalogenowany	PE
Materiał przewodu wewnętrznego	Drut aluminiowy pokryty miedzią
Materiał taśmy ochronnej	Aluminium
Minimalny promień gięcia, pojedyncze gięcie	25,4 mm
Temperatura instalacji	-40 °C to +85 °C
Temperatura pracy	-40 °C to +85 °C
Temperatura przechowywania	-70 °C to +85 °C

1.5 Konfiguracja punktów logicznych

Punkt logiczny PEL oparty został na jednym uniwersalnym ekranowanym gnieździe teleinformatycznym (z możliwością wymiany interfejsu końcowego w postaci wkładki, bez zmian w trwałym zakończeniu kabla na złączu), oraz dwóch gniazdach modularnych RJ45, montowanych w uchwycie do osprzętu 45x45mm.

Wymagania gniazda dla systemu okablowania otwartego

Wymaga się aby gniazda teleinformatyczne (stanowiące trwały element zakończenia kabla) posiadały wydajność transmisyjną o co najmniej 25% większą. Jest to spowodowane faktem, że gniazdo teleinformatyczne jest kluczowym elementem całego systemu i zapewnienie jego

wymaganej wydajności gwarantuje niezależność i pewność uzyskania pozytywnych wyników pomiarów w przypadku nawet niedokładnej instalacji lub błędów w ułożeniu kabla.

Zestaw instalacyjny powinien zawierać płytę czołową prostą z ramką montażową 45mm, ekranowaną puszkę instalacyjną (wymagany kontakt ekranu kabla i obudowy złącza po całym obwodzie kabla - 360°) z wyprowadzeniem kabla do góry, w lewo lub prawo oraz wyposażoną w złącze modułarne o wydajności min. kat.7A. Dodatkowo powinny znajdować się zaciski umożliwiające optymalne wyprowadzenie kabla i kontakt ekranu oraz etykieta opisowa. Gniazda logiczne należy montować podtynkowo w puszkach, w uchwycie do osprzętu (45x45). Należy zapewnić puszki o głębokości minimum 60mm lub większej, przeznaczone do osprzętu z uchwytem 45x45 i zapewniające odpowiednią ilość miejsca dla zapasu kabla, który ma być zwinięty w puszcze instalacyjnej.

Kabel transmisyjny S/FTP kat.7 zgodny ze specyfikacją projektową należy zakończyć na uniwersalnym ekranowanym złączu 8-pozycyjnym, akceptującym drut miedziany o średnicy 0,50 - 0,65mm (24 - 22 AWG). Proces zarabiania kabla na uniwersalnym złączu 110 wymaga zastosowania standardowego narzędzia tzw. uderzeniowego lub narzędzia do złączy LSA+. Dopuszczalne jest zastosowanie do montażu narzędzi, które w jednym ruchu terminują trwale wszystkie (wcześniej przygotowane) żyły kabla transmisyjnego na całym 8-pozycyjnym złączu modułarnym. Do montażu można wykorzystać uchwyt montażowy i wzornik długości oraz rozmieszczenia par kabla, a w celu uzyskania właściwego dostępu także narzędzie do otwierania tylnej pokrywy gniazda. Należy zwrócić uwagę na zakończenie indywidualnych ekranów par transmisyjnych. Proces montażu ma powtarzalnie gwarantować najwyższe parametry – w tym celu maksymalny rozplot par transmisyjnych na ekranowanym uniwersalnym złączu modułarnym 110 nie może być większy niż 6 mm. Taki zespół należy umieścić w ekranowanej obudowie/składanej puszcze Faraday'a z automatycznym, tzn. sprężynowym 360° uchwytem ekranu kabla.

Ze względu na dostępne obecnie na rynku urządzenia aktywne dla zapewnienia pełnej kompatybilności wstecz na etapie uruchomienia instalacji wymaga się zastosowania interfejsu RJ45.

Wybór interfejsu kończącego kabel zależy od zastosowanej odpowiedniej wkładki wymiennej wkładanej do uniwersalnego ekranowanego złącza modułarnego. **W celu prawidłowej konfiguracji torów transmisyjnych po obydwu stronach łącza należy stosować takie same wkładki wymienne.**

Gniazdo w konfiguracji podstawowej w momencie uruchomienia instalacji należy wyposażać we wkładki pojedyncze typu 1xRJ45 kat.6A. Docelowa wydajność systemu jest wyższa, zgodnie z wcześniejszymi wymaganiami.

Wymagania gniazda dla systemu okablowania modułarnego

Wszystkie gniazda mają być zakańczane za pomocą narzędzi np. nożem uderzeniowym lub narzędziem, które pozwala zakończyć wszystkie pary w jednym ruchu i z jednakową siłą. Celem jest

zachowanie minimalnego rozplotu par nie większego niż 6mm i w efekcie uzyskanie wysokich zapasów parametrów transmisyjnych. Jednocześnie odrzuca się wszelkie gniazda zarabiane beznarzędziowo, które nie spełniają powyższego opisu.

Wymagane jest, aby producent przedstawił certyfikaty pomiarowe niezależnych akredytowanych laboratoriów na zgodność z parametrami kategorii 6A do 500MHz dla wszystkich gniazd kat. 6A przeznaczonych do zabudowy zgodnie ze specyfikacją PN-EN 50173-1 lub ISO/IEC11801.

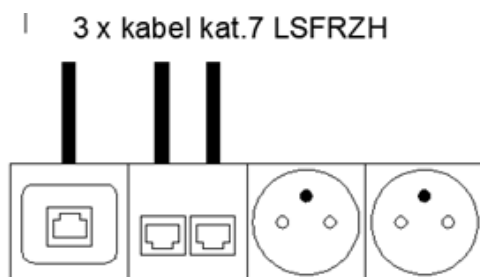
Moduł gniazda RJ45 ma posiadać pełne ekranowanie i konstrukcję dwuelementową, składającą się z części przedniej (z interfejsem RJ45 oraz złączami IDC dla par transmisyjnych i bocznymi ostrzami do odcięcia ich nadmiaru w trakcie zarabiania złącza) oraz części tylnej (zintegrowanej prowadnicy par transmisyjnych wraz z sprężynowym samozaciskowym uchwytem 360o kabla ekranowanego na całym obwodzie kabla). Ekranowana, asymetryczna metalowa obudowa (w formie odlewu, zarówno na części przedniej i tylnej) podczas montażu gniazda ma się składać w szczelną całość, tworząc zintegrowaną i szczelną klatkę Faradaya, zabezpieczoną konstrukcyjnie nawet przed zakłóceniami pochodzącymi od modułów gniazd zainstalowanych w jednym rzędzie. Konstrukcja modułu i uchwytu ekranu nie może zniekształcać konstrukcji kabla, ma również zapewniać maksymalną łatwość instalacji oraz gwarantować najwyższe parametry transmisyjne. Wymaga się, aby każdy moduł gniazda RJ45 posiadał możliwość uniwersalnego terminowania kabli, tj. w sekwencji T568A lub T568B. Każdy moduł ma być zarabiany narzędziami. Zalecane jest, wykorzystanie do montażu takich narzędzi, które poprzez jeden ruch narzędzia, zapewniają krótkie rozploty par – max. 6mm (a przez to najlepsze możliwe osiągi transmisyjne) oraz dużą powtarzalność i szybkość zarabiania. System okablowania strukturalnego ma zapewniać pełne wsparcie dla standardu 802.3af (PoE+) przy zachowaniu żywotności gniazd wynoszącym minimum 750 cykli połączeniowych (tj. utrzymaniu wymaganych minimalnych parametrów elektrycznych i transmisyjnych), co musi być potwierdzone przez testy wykonane przez producenta lub certyfikaty wystawione przez niezależne laboratoria.

Moduł gniazda ekranowanego o wydajności 500 Mhz kategorii 6A, ma być zarobiony przy zastosowaniu profesjonalnego narzędzia montażowego. Pomiar takiego toru charakteryzuje się wysoką powtarzalnością wyniku z uwagi na mały wpływ człowieka, który w dużej części zastąpiony jest półautomatycznym narzędziem. Wykorzystanie powyższej metody terminowania złącz jest najnowszym trendem proponowanym przez największych liderów w rynku okablowania strukturalnego. Moduły ekranowane gniazd RJ45, mają umożliwiać terminację drutu miedzianego średnicy od 26 – 22 AWG. Charakterystyka transmisyjna modułu gniazda RJ45 ma być potwierdzona przez certyfikaty wystawione przez niezależne akredytowane laboratorium i testów przeprowadzonych w paśmie częstotliwości do minimum 500HMz, zgodnie z wymaganiami transmisyjnymi norm specyfikujących Klasę EA/Kategorię 6A .Dodatkowo moduł musi posiadać możliwość oznaczenia kolorem do różnych zastosowań: WIFI, CCTV, KD itp w celu łatwej administracji dla Użytkownika systemu.

1.5.1 Konfiguracja punktu logicznego PEL

Punkt logiczny PEL należy wykonać podtynkowo i ma składać się z jednego gniazda logicznego systemu otwartego oraz dwóch gniazd logicznych systemu modularnego. Wszystkie gniazda w punkcie PEL mają być wyposażone na etapie wykonania instalacji w interfejs RJ45 kat.6_A. Do punktu logicznego PEL należy doprowadzić 3 kable typu S/FTP kat. 7 zgodnie ze specyfikacją okablowania poziomego. Gniazda logiczne mają zostać zainstalowane zgodnie z rysunkiem 1.

Rys. 1. Punkt Logiczny PEL



1.5.2 Konfiguracja punktu logicznego PL

Punkt logiczny PL należy wykonać w postaci gniazda modularnego RJ45 kat.6_A. PL ma składać się z 1 gniazda logicznego. Do punktu logicznego PL należy doprowadzić jeden kabel typu S/FTP kat. 7 zgodnie ze specyfikacją okablowania poziomego.

Punkt PL dedykowany jest do obsługi systemów bezpieczeństwa KD, CCTV, SSP i SSWIN. Moduł RJ45 należy zatem umieścić w odpowiedniej dla systemu obudowie/puszcze instalacyjnej, a urządzenia końcowe podłączyć za pomocą odpowiedniego kabla krosowego.

Wymagania dla kabli

Wymagania dla kabli S/FTP kat.7

Ze względu na przyjęte założenia instalacyjne oraz sposób prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 7,3 mm (co determinuje maksymalną średnicę żyły na 23AWG). Nie dopuszcza się kabli o większej średnicy zewnętrznej.

Instalacja ma być poprowadzona ekranowanym kablem konstrukcji S/FTP z osłoną zewnętrzną trudnopalną (LSZH). Ekran takiego kabla ma być zrealizowany na dwa sposoby:

1. w postaci jednostronnie laminowanej folii aluminiowej oplatającej każdą parę transmisyjną (w celu redukcji oddziaływań między parami),

2. w postaci wspólnej siatki okalającej dodatkowo wszystkie pary (skręcone razem między sobą) – w celu redukcji wzajemnego oddziaływania kabli pomiędzy sobą.

Taka konstrukcja pozwala osiągnąć najwyższe parametry transmisyjne, zmniejszenie przesłuchu NEXT i PSNEXT oraz zmniejszyć poziom zakłóceń od kabla. Pozwala także w dużym stopniu poprawić odporność na zakłócenia zarówno wysokich, jak i niskich częstotliwości. Kabel musi spełniać wymagania stawiane komponentom przez najnowsze obowiązujące specyfikacje.

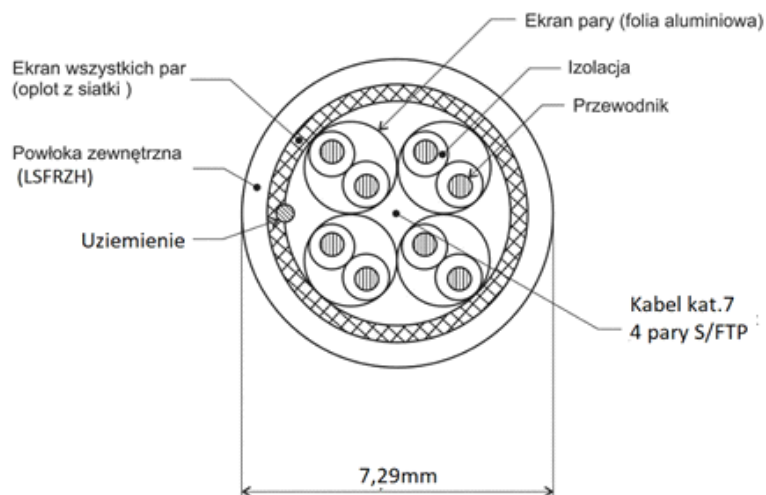
Proces montażu ma gwarantować najwyższą powtarzalność. Maksymalny rozplot pary transmisyjnej na złączu modularnym (umieszczonych w zestawach instalacyjnych) nie może być większy niż 6 mm.

Kabel ten ma spełniać wymagania stawiane komponentom Kategorii 6A przez obowiązujące specyfikacje norm, równocześnie zapewniając pełną zgodność z niższymi kategoriami okablowania.

Tabela 2 Wymagania dla kabla systemu okablowania strukturalnego (S/FTP Kat.7)

Budowa kabla	S/FTP (zgodnie z rysunkiem)
Wydajność kabla	Kategoria 7 wg. ISO/IEC 11801; EN 50173-1 z charakterystykami rozszerzonymi do częstotliwości 1000MHz
Certyfikat	Producent musi dostarczyć certyfikat wydany przez laboratorium potwierdzający jego charakterystyki na kategorię 7
Normy dotyczące palności	IEC 60332-1, IEC 60754-1, IEC 60754-2, IEC 61034-2
Tłumienie sprzężenia	Typ 1
Średnica zewnętrzna kabla	max.7,29 mm
Napężenie podczas instalacji	≤110N
Średnica przewodnika	23AWG
Impedancja	100 ohm
Tolerancja impedancji	±15 ohm
Klasa segregacji elektromagnetycznej	d
Rezystancja dc max.	15 ohms/100 m
Współczynnik propagacji NVP	Min. 80%

Temperatura instalacji	podczas	Minimum przedział 0°C do +50°C
Temperatura instalacji	podczas	Minimum przedział -20°C do +60°C
Ośłona zewnętrzna:		LSFRZH
EN50575 CPR EuroClass		Dca
EN50575 CPR EuroClass		s2
EN50575 CPR EuroClass		d1
EN50575 CPR EuroClass		a1
REACH-SVHC / EU REACH SVHC - 1907/2006/EC : 2016-06-20		Zgodne
EU RoHS - 2011/65/EU : 2015-03-31		Zgodne



Rys. 2 Budowa kabla kat. 7 S/FTP

Tabela 3 Wymagania dla parametrów transmisyjnych kabla systemu okablowania przy częstotliwościach kluczowych

Częstotliwość	Tłumienie	ACR	PSNEXT	RL
[MHz]	[dB]	[dB]	[dB]	[dB]
450	39	39	85	26

600	46	34	77	25
750	52	28	75	24
900	55	17	72	23
1000	57	15	70	20

1.2 Kable krosowe miedziane

Kable obszaru roboczego (przyłączane do stacji użytkownika), jak i krosowe (w szafie kablowej) mają być fabrycznie wykonane z linki ekranowanej S/FTP - 500MHz w osłonie LSZH. Wtyk złącza RJ45 ma posiadać szczelną elektromagnetycznie osłonę ekranowaną, tak aby zapewnić kontakt elektryczny z obudową ekranowanych gniazd RJ45 po całym obwodzie złącza. Wymaga się standardowej sekwencji rozszycia kabla T568B (preferowana) lub T568A. Osłona zewnętrzna kabli ma być typu LSZH.

Wszystkie kable obszaru roboczego i krosowe mają być fabrycznie wykonane i testowane. Wszystkie komponenty składowe: wtyki, kabel mają być wyprodukowane i trwale oznaczone przez tego samego producenta co cały system okablowania. Kable krosowe miedziane mają być zgodne ze specyfikacją Kat.6A.

Ze względu na dużą gęstość połączeń i duże upakowanie wszystkie kable krosowe stosowane w obrębie Głównego Punktu Dystrybucyjnego mają mieć grubość żyły nie większą niż AWG 30 i średnice kabla nie większą niż 4,5 mm, natomiast kable obszaru roboczego grubość żyły nie większą niż AWG 26/7 i średnice kabla nie większą niż 6,3 mm.

1.3 Wymagania dotyczące paneli krosowych

Wymagania paneli dla systemu okablowania otwartego

Kable transmisyjne systemu otwartego należy zakończyć na panelach krosowych 24 portowych, zawierających uniwersalne gniazda z ekranowanymi złączami modularne typu 110 o wydajności min. kat.7A. Konstrukcja portów – czyli uniwersalnych gniazd ma być adekwatna do konstrukcji i funkcjonalności opisanych wcześniej gniazd naściennych w systemie otwartym i zawierać ekranowane złącze szeregowo i pełną klatkę Faraday’a z automatycznym-sprężynowym mechanizmem mocującym kabel), z tym że gniazda mają być zblokowane w 2-gniazdowe zespoły, idealnie odzwierciedlające Zespoły przyłączeniowej w Punktach Logicznych PEL. Kable wyprowadzane z gniazd – portów panela „na wprost” – pod kątem 180° należy wesprzeć na tylnej prowadnicy panela, mocując je lekko za pomocą opasek kablowych, zaś sam panel uziemić

wykorzystując zacisk uziemiający obecny na prowadnicy tylnej. Panel dodatkowo należy wyposażać w przednie wieszaki po obydwu stronach, co wymusza naturalny kierunek wyprowadzenia kabli krosujących na boki szafy.

W uniwersalnym ekranowanym panelu wyposażonym w złącza modułowe, można umieścić dowolne wymienne wkładki, o wymaganej wydajności (kategorii okablowania) i z odpowiednim interfejsem końcowym. W momencie uruchomienia instalacji, w portach panela należy umieścić wkładki pojedyncze typu 1xRJ45 kat.6A. Docelowa wydajność systemu jest wyższa, zgodnie z wcześniejszymi wymaganiami.

Wymagania paneli dla systemu okablowania modułowego

Kable należy zakończyć na modułowym panelu krosowym o wysokości montażowej 1U o konstrukcji kątovej z płytą czołową cofniętą względem płaszczyzny montażu w stelażu, aby gniazda nie wystawały przed płaszczyznę stelaża rack. Panel musi posiadać możliwość montażu 24 oddzielnych modułów RJ45 typu SL, co zapewni łatwy montaż, terminowanie kabli oraz uniwersalne rozszycie kabla w sekwencji T568A lub T568B, przy czym każdy port ma mieć możliwość oddzielnego opisu i oznaczenia poprzez system kolorowych ikon. Kable instalacyjne, zakańczane na panelu, należy – w celu zapewnienia optymalnego prowadzenia – wesprzeć na prowadnicy kabli, montując je za pomocą opasek kablowych (należy zwrócić uwagę, aby zbyt mocno nie zaciskać opasek; mają one tylko lekko utrzymać kabel na prowadnicy).

1.4 Punkt Dystrybucyjny

W szafach dystrybucyjnej należy zainstalować osprzęt połączeniowy oraz sprzęt aktywny.

Szafa ma posiadać stopień ochrony przynajmniej IP20 zgodnie z PN 92/E-08106 /EN 60 529 / IEC 529.

Uwaga: Ulokowanie szaf zostało pokazane na podkładach dołączonych do projektu oraz na schemacie ideowym okablowania strukturalnego.

Dokładne zestawienie wyposażenia szaf oraz zestawienie ilościowe sprzętu instalowanego w szafach znajduje się w zestawieniach materiałowych dołączanych do projektu.

Przed montażem sprzętu w szafie należy sprawdzić czy jest wymagana odległość stelaża od drzwi szafy do montażu wieszaków - jeżeli nie należy przesunąć stelaże. Sprzęt należy instalować zgodnie z rozmieszczeniem zaproponowanym na rysunkach dołączonych do projektu. Okablowanie poziome oraz szkieletowe należy wprowadzać do szaf od góry poprzez otwór powstały przez wyciągnięcie dekła maskującego. W określonych przypadkach należy zbudować trasę kablową tak, aby kable nie były narażone na uszkodzenia wynikające z długotrwałych naprężeń.

W szafach bezwzględnie należy zostawiać zapas instalacyjny kabla.

Wymagania dla szafy GPD

- § Wysokość 42U, szerokość 800mm oraz głębokość 1000 mm;
- § Cztery pionowe profile / słupy montażowe o rozstawie 19”;
- § Drzwi przednie dwuskrzydłowe perforowane 80% z zamkiem i klamką;
- § Drzwi tylne dwuskrzydłowe perforowane 80% z zamkiem i klamką;
- § Ściany boczne zdejmowane;
- § Perforacja u dołu szafy na wszystkich ścianach;
- § 2 pary regulowanych belek montażowych z numeracją, wykonanych z blachy ocynkowanej w rozstawie 19;
- § Wszystkie elementy rozłączne tj. drzwi, ściany boczne itd. mają posiadać linki uziemiające;
- § W dachu i podstawie otwory pod zainstalowanie paneli wentylacyjnych/zaślepek z włókniną oraz otwory umożliwiające wprowadzenie kabli liniowych od góry;
- § Dół szafy wypełniony panelami zasłepiającymi otwory do wprowadzenia kabli od dołu;
- § Otwór o wysokości min. 3U i szerokości min 450mm znajdujące się w dolnej części tylnej ściany szafy;
- § Szafa ma posiadać nóżki regulowane lub możliwość zastosowania kół jezdnych
- § Szafa musi być wypoziomowana.
- § Nośność min. 1200 kg

❑ Materiał: blacha alucynkowo-krzemowa z katodową ochroną antykorozyjną

1.5 System organizacji połączeń w szafie GPD

System zarządzania połączeniami został zaprojektowany specjalnie w tej konfiguracji, by w pełni zapanować, ogarnąć i ułatwić administrację nad wszystkimi maksymalnie zagęszczonymi połączonymi elementami całego systemu. Zwiększona o ok. 40% gęstość połączeń została osiągnięta

przez zastosowanie elementów prowadzących, które gwarantują zachowanie optymalnych promieni zagięcia zainstalowanych kabli połączeniowych (miedzianych lub światłowodowych).

Kątowe wyprowadzenia kabli z paneli i urządzeń aktywnych na zoptymalizowanej pod tym kątem konstrukcji wsporników, redukuje naprężenia kabli, organizuje w sposób uporządkowany ich zagęszczenie i pozwala na lepsze zarządzanie kablami z stworzenia w pełni kontrolowanych wiązek kabli krosowych.

Ze względu na duże zagęszczenie połączeń prowadnice kątowe należy zastosować dla pełnego wyposażenia szaf krosowych oraz urządzeń aktywnych.

Dodatkowo we wszystkich nieobsadzonych miejscach szafy należy doposażyć w poziome prowadnice kablowe 1U dla pełnego obsadzenia szafy na pełną wysokość 42U.



Rys. 3 Przykładowa konstrukcja wieszaka kątowego

1.6 Listwa PDU i monitoring środowiska

1.6.1 Listwa PDU

Listwy PDU monitorują zasilanie w serwerowni i warunki środowiskowe na poziomie szafy, poprzez ciągłe skanowanie potencjalnych przeciążeń obwodów elektrycznych i parametrów dotyczących otoczenia które mogłyby spowodować uszkodzenie kosztownego sprzętu IT. PDU muszą dostarczać wszechstronnych, dokładnych pomiarów energii użytej do zasilania sprzętu IT w celu efektywnego wykorzystania zasobów. Należy odpowiednio dobrać PDU, sensory środowiskowe i zabezpieczonych kabli zasilających aby spełnić wymagania dotyczące bezpieczeństwa i zarządzania dla nowoczesnych środowisk Serwerowni.

Tabela 4 Listwy PDU stosowane w projekcie

Szafa	Ilość PDU	Ilość faz w PDU	Prąd wejściowy na fazę	Orientacja		Moc pozorna	Gniazda C13 – minimalna wymagana ilość	Gniazda C19 – minimalna wymagana ilość
GPD	1	1	16A	Pionowa		3,7(kVA)	20	4

Listwy dla dystrybucji zasilania w szafach PDU muszą spełniać poniższe wytyczne:

- § Zgodność z normami:
- § ANSI/TIA-569-D Telecommunications Pathways and Spaces, 2015;
- § ANSI/NFPA 70 – National Electric Code, 2008, 2014;
- § 2014/35/EU – Low Voltage Directive;
- § 2014/30/EU – Electromagnetic Compatibility Directive;
 - § 2011/65/EU – Restriction of use of certain hazardous substances in electrical and electronic equipment directive (RoHS2);
 - § EN 55032:2015 – Information technology equipment. Radio disturbance characteristics. Limits and method of measurement;
 - § EN 55024:2010 – Information technology equipment. Immunity characteristics. Limits and methods of measurement;
 - § EN 60950-1: 2006/A11:2009/A1:2010/A12:2011/A2:2013 – Information technology equipment. Safety. General requirement;
- § EN 50600-2-2: Data Center Electrical Power Distribution;
- § Certyfikat - FCC Rules Part 15 – EMC Verification, Canadian ICES-003;
 - § Producent musi oferować listwy PDU zarówno w wersji montażu pionowej jak i poziomej 19”;
 - § PDU muszą wytrzymać temperaturę do 60°C przy pełnym obciążeniu na wszystkich gniazdach;
 - § PDU o dużej gęstości upakowania gniazd (do 48 sztuk) na jednym profilu o wymiarach max. 1821.2mm x 50.8mm x 111.8mm (musi zmieścić się do szafy 42U) dla zminimalizowania przestrzeni i zmaksymalizowania przepływu powietrza w szafie;
- § Szerokość listw pionowych max. 50,8mm;
 - § Możliwość wymiany kontrolera z wyświetlaczem w trakcie pracy listwy PDU (Hot-Swap);
 - § Kontroler PDU z wyświetlaczem musi mieć możliwość obrotu o 180° w zależności od strony na której jest montowana listwa;
 - § Kontroler musi posiadać jasny wyświetlacz OLED z wysokim współczynnikiem kontrastu;
 - § Redundantny dostęp sieciowy 1Gb/s w konfiguracji 2N dla redundancji połączeń w sieci lub połączeniu do sieci różnych użytkowników;
 - § Przełączanie gniazd zasilających i krytycznych funkcji PDU musi odbywać się za pośrednictwem HTTPS/TLS, a nie SSL;
 - § Musi być obsługiwane bezpieczne monitorowanie sieci, aby uniknąć wtargnięć - cała komunikacja danych powinna obsługiwać bezpieczne funkcje RESTful API przez HTTPS/TLS z wykorzystaniem otwartego, niezastrzeżonego standardu branżowego;
 - § Musi obsługiwać standard Redfish API;
 - § Gniazda zasilające muszą obsługiwać najnowsze zabezpieczenia i spełniać rygorystyczne wymagania bezpieczeństwa narzędzi do skanowania;
 - § HPE WebInspect Security;

- § Tenable Nessus;
- § DDI Frontline;
- § BackTrack Linux Security Editor;
- § PDU musi obsługiwać kodowane oznaczone kolorami gniazda C13/C19 w celu identyfikacji każdej z 3 faz z kolorowymi bezpiecznikami automatycznymi;
- § PDU musi być dostępne przynajmniej w 6 kolorach do wyboru w celu łatwej identyfikacji i zarządzania zasilaniem w szafach;
 - PDU musi obsługiwać połączenie sieciowe 1Gb/s i umożliwiać połączenie do 4 listw PDU w celu oszczędzania adresów IP;
- § Montaż listw PDU musi odbywać się bez użycia narzędzi i umożliwiać regulowanie położenia jednostki PDU;
- § Graficzny interfejs użytkownika jednostki PDU musi dostosowywać się do rozdzielczości ekranu urządzenia użytkownika w celu uzyskania optymalnego interfejsu na urządzeniach mobilnych i tabletach;
- § Kodowane gniazda IEC są kompatybilne z bezpiecznymi kablami zasilającymi z blokowaniem W i V z dodatkowym zabezpieczeniem za pomocą standardowych opasek kablowych;
- § Minimum 3-letnia standardowa gwarancja producenta z możliwością rozszerzenia do 5-lat;
- § Skalowalność pod względem zarządzania urządzeniem za pomocą lokalnego serwera WWW do systemu DCIM w celu monitorowania energii i mocy u jednego dostawcy;
- § Obsługa portu USB umożliwiającego szybkie instalowanie oprogramowania wbudowanego i poprawek zabezpieczeń bez wyłączania niezgodnych urządzeń w sieci;
- § Musi istnieć możliwość wyłączenia portu USB do udostępniania za pomocą blokady programowej w celu ochrony przed włamaniami;
- § Monitorowanie zużycia energii z dokładnością do +/-1% zapewniające dokładność rozliczeniową zgodnie ze specyfikacjami IEC;
- § Pomiary muszą obejmować odczyty V, A, VA, W, kWh i PF;
- § Obsługa wysokiej niezawodności hydrauliczno-magnetycznych wyłączników awaryjnych stabilnych w temperaturze do min.60°C;
- § Oferowany asortyment listw PDU musi zawierać możliwość elastycznego zastosowania odpowiedniej listwy w zależności od potrzeb klienta m.in.:
 - § Niemonitorowanych listw (NM);
 - § Monitorowane Wejścia (MW) - jednostka PDU z możliwością monitorowania potencjalnej agregacji mocy po to aby szybko zidentyfikować potencjalne problemy z zasilaniem i odzyskać dostępną lub niewykorzystaną moc;
 - § Monitorowane Przełączanie (MP) – jednostka PDU z możliwością monitorowania potencjalnej agregacji mocy i przełączania poziomu wyjściowego na poszczególne gniazda lub grupę gniazd. Umożliwia sekwencjonowanie mocy, ponowne uruchomienie sprzętu lub ograniczenie nieuprawnionego użycia gniazda zasilającego;
 - § Monitorowanie na poziomie indywidualnego Gniazda (MG) – jednostka PDU z możliwością monitorowania mocy wyjściowej, aby szybko zidentyfikować potencjalne problemy z zasilaniem oraz odzyskać dostępną lub niewykorzystaną moc wyjściową na

poziomie gniazd, umożliwiając ponowne przegrupowanie lub wyłączenie poszczególnych serwerów w celu odzyskania dostępnej lub niewykorzystanej mocy;

§ Monitorowanie i Przełączanie na poziomie indywidualnego Gniazda (MPG) – jednostka PDU z możliwością monitorowania mocy wyjściowej i możliwości przełączania poziomu wyjściowego dla poszczególnych gniazd lub grupy gniazd. Monitorowanie mocy na poziomie indywidualnego gniazda zapewnia praktyczne dane dotyczące zarządzania zużyciem energii każdego podłączonego urządzenia IT, umożliwiając ponowne przegrupowanie lub wyłączenie poszczególnych serwerów w celu odzyskania dostępnej lub niewykorzystanej mocy;

§ Spełnia globalne standardy zgodności zasilania: UL, cULus, CE i EAC;

§ Obsługa monitorowania rozgałęzionych obwodów i równoważenia obciążenia każdego obwodu;

§ Obsługa gniazd naprzemiennych;

§ Wyświetlanie wszystkich trzech faz jednocześnie na wyświetlaczu OLED podczas ręcznego gromadzenia danych;

§ PDU musi natywnie obsługiwać różne czujniki i rozwiązania kontroli dostępu za pośrednictwem tej samej jednostki PDU bez zewnętrznego urządzenia bramowego;

§ Dostawca PDU musi dostarczać cyfrowe czujniki środowiskowe oraz bezpieczeństwa m.in.:

§ Temperatury;

§ Temperatury + wilgotności;

§ 3x temperatura + wilgotność;

§ Liniowy czujnik zasilania;

§ Punktowy czujnik zasilania;

§ Wejście styku bez potencjałowego;

§ Kontaktron drzwiowy;

§ HUB dostępowy dla kontroli dostępu do szafy (wymagana obsługa technologii kart 125kHz i 13,56MHz);

§ Listwa oświetleniowa LED;

§ HUB rozszerzenia portów sensorów

§ Obsługa interfejsu bezprzewodowego za pomocą klucza sprzętowego sieci bezprzewodowej;

Tabela 5 Parametry elektryczne listw PDU

Napięcie wejściowe	Jednofazowe PDU – 240V
Prąd wejścia (na fazę)	16A
Moc wejściowa	3,7(kVA)
Częstotliwość wejściowa	50/60Hz

Napięcie wyjściowe	120-240VAC
Maksymalny prąd wyjściowy (gniazdo)	IEC C13: 10A
	IEC C19: 16A
	NEMA 5-20R: 16A
Zabezpieczenie przed przeciążeniem (jeśli dotyczy)	Zabezpieczenia hydrauliczno-magnetyczne

Tabela 6 Parametry ogólne listw PDU

Temperatura pracy	10°C do 60°C
Temperatura przechowywania	-20°C do 60°C
Wilgotność względna: Podczas pracy	10% do 90% bez kondensacji
Wilgotność względna: Bez działania	5% do 95% RH
Wilgotność względna: Przechowywanie	5% do 95%
Wysokość podczas pracy	0 – 3000m
Wysokość podczas przechowywania	0 – 9144m
Zgodność ze standardami	CE
Zgodność środowiskowa	RoHS & REACH

1.6.2 Monitoring środowiska

Czujniki temperatury i wilgotności

Czujniki powinny zawierać:

- wbudowany mikrochip, który konwertuje sygnały analogowe na format cyfrowy, zanim dane dotrą do PDU;
- bezpośrednie połączenie z PDU za pomocą dostarczonego standardowego kabla sieciowego;
- szybkozłącze i kabel Ethernet;

Tabela 7 Specyfikacja czujnika temperatury i wilgotności

	Temperatura i wilgotność
--	--------------------------

Elektryczne	
Napięcie robocze	5V DC
Skala	0°C~+65°C, wilgotność względna 10–90%, bez kondensacji
	±2°C
Precyzja	±5% RH w 5-50°C
	10 ~ 90% RH
Typ przewodu (od PDU do puszki czujnika)	Patchcord kat. 5, UTP
Fizyczne	
	2m (od PDU do puszki czujnika)
Długość	1m (czujnik temperatury T1/T3 do puszki czujnika)
Środowiskowe	
Wysokość n.p.m (eksploatacja przechowywanie)	0-3048m/0-15240m
Temperatura (Obsługa przechowywanie)	0°C~+70°C/-20~+70°C
Wilgotność (Obsługa przechowywanie)	0-95% RH, bez kondensacji
Weryfikacja środowiskowa	ROHS, WEEE

1.7 Urządzenia aktywne

Całość dostarczanego sprzętu, łącznie z akcesoriami i oprogramowaniem musi być fabrycznie nowa, nie używana we wcześniejszych projektach. Zamawiający wymaga zapewnienia warunków bezpłatnej dożywotniej gwarancji. W celu obniżenia kosztów użytkowania i posiadania urządzeń oraz podniesienia i kontroli poziomu bezpieczeństwa, a także możliwości wyboru i łatwej rekonfiguracji parametrów transmisyjnych wymaga się aby dostarczane przełączniki gwarantowały jednorodność rozwiązania i możliwość zarządzania za pomocą jednolitej platformy oprogramowania. Platforma ta ma służyć do zarządzania siecią z poziomu komputerów PC, umożliwiać odwzorowywanie, konfigurowanie i monitorowanie stanu połączeń. Ma przy tym

zapewniać podstawowe funkcje bezpieczeństwa (do szyfrowanej komunikacji i pokonywania zapory) i możliwość rozbudowy sieci różnych wielkości ze zdalnymi ośrodkami. Kontrola zarządzania w skali całej sieci ma pozwalać użytkownikom bezpiecznie dodawać, dostosowywać i ograniczać prawa dostępu do zarządzania siecią, a także zapewniać funkcje bezpieczeństwa i być zgodna z technologiami i urządzeniami do transmisji bezprzewodowych. Oprogramowanie ma oferować jednopanelową możliwość zarządzania i mieć możliwość rozbudowy o tzw. agentów zdalnych.

Tabela 8 Parametry wymaganego przełącznika sieci LAN :

Porty i sloty	48 portów RJ-45 10/100/1000 z automatycznym wykrywaniem (IEEE 802.3 typ 10BASE-T, IEEE 802.3u typ 100BASE-TX, IEEE 802.3ab typ 1000BASE-T); Duplex: 10BASE-T / 100BASE-TX: half or full; 1000BASE-T: full only 4 SFP+ 1/10GbE ports; PHY-less
Dodatkowe Porty i sloty	1 dual-personality (RJ-45 or USB micro-B) port konsoli
Waga	6.83 lb (3.10 kg)
Pamięć i procesor	Dual Core ARM Cortex @ 1016 MHz, 1 GB DDR3 SDRAM; Packet buffer size: 12.38 MB 4.5MB Ingress/7.875MB Egress, 4 GB eMMC
Wydajność	1000 Mb Latency < 3.8 μ s (64-byte packets) 10 Gbps Latency < 2.9 μ s (64-byte packets) Przepustowość: do 112.0 Mpps Przełączanie: 176 Gbps Rozmiar tablicy routingu: 2,000 IPv4, 1,000 IPv6 in hardware, 200 OSPF, 256 Static, 10,000 RIP Rozmiar tablicy adresów MAC: 32768 entries
Środowisko	Temperatura robocza: 0°C do 45°C; Wilgotność: 15% do 95% @ 40°C, bez kondensacji

	Temperatura przechowywania: -40°C do 70°C Poziom hałas: Moc: 54,1 dB, Ciśnienie: 40,2 dB Wyrzut ciepłego powietrza: na boki Wydzielane ciepło: 157.2 BTU/hr (165.8 KJ/hr)
Elektryczność	Napięcie zasilania: 100 - 127 / 200 - 240 VAC Prąd: 0.9/0.6 A Maksymalna moc znamionowa: 46.6 W
Bezpieczeństwo	UL 60950-1, 2nd Edition; UL 62368-1: 2nd Edition; EN 60950-1:2006 +A11:2009 +A1:2010 +A12:2011+A2:2013; IEC 60950-1:2005 +A1:2009 +A2:2013; EN 62368-1: 2nd Edition; CSA 22.2 No. 60950-1-07 2nd; IEC-62368-1: 2nd Edition; EN 60825-1:2014 / IEC 60825-1:2014 Class 1
Emisyjność	EN 55032:2012/CISPR 32 Class A; FCC CFR 47 Part 15 Class A; VCCI Class A; ICES-003 Class A; CNS 13438
Odporność	Ogólne EN 55024: 2010 / CISPR 24 ESD IEC 61000-4-2 Promieniowane IEC 61000-4-3 EFT / Burst IEC 61000-4-4 Przepięcie IEC 61000-4-5 Porażenie IEC 61000-4-6 Pole magnetyczne o częstotliwości sieciowej IEC 61000-4-8 Spadki i przerwy napięcia IEC 61000-4-11 Harmoniczne IEC / EN 61000-3-2 Wahania napięcia IEC/EN 61000-3-3
Zarządzanie	Przełącznik zarządzalny min. na poziomie L2/L3 z obsługą VLAN 802.1q, ACL na poziomie L3/L4, routingu IP i min. 4 strefami

	bezpieczeństwa (VLAN)
Port security	Tak, dla poszczególnych portów
Trunking 802.1q	Tak
Obsługa RST (802.1w), PVRST	Tak
Obsługa MSTP (802.1s)	Tak
Obsługa IGMP snooping	Tak
Obsługa agregacji portów (802.3ad/LACP)	Tak
Obsługa ramek Jumbo	Tak, do min. 9216 bajtów
Funkcjonalność Strom control (unicast, multicast i broadcast)	Tak
Funkcjonalność PVLAN lub analogicznej (np. Port isolation)	Tak
Autoryzacja w oparciu o 802.1x z możliwością dynamicznego przypisania użytkownika do VLAN i ACL	Tak
Uwierzytelnienie urządzeń w oparciu o adres MAC	Tak
Funkcjonalność suplikanta 802.1x	Tak
Funkcjonalność Port security	Tak
Funkcjonalność DHCP Snooping	Tak
Funkcjonalność Dynamic ARP Inspection	Tak
Funkcjonalność IP Source Guard	Tak
Autoryzacja prób logowania do urządzenia na serwerach RADIUS lub TACACS+	Tak
Funkcjonalność STP Root guard	Tak
Funkcjonalność STP Port	Tak
Implementacja min. 4 kolejek dla ruchu wyjściowego na każdym porcie dla ruchu o różnej klasie oraz implementacja algorytmu Shaped Round Robin lub podobnego do obsługi tych kolejek oraz	Tak

możliwość obsługi jednej z tych kolejek z bezwzględnym priorytetem (Strict Priority)

Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie adresów MAC, IP lub portów TCP

Tak

Współpraca z serwerem Syslog

Tak

Liczniki pakietów wchodzących/wychodzących dla każdego portu

Tak

Tekstowy plik konfiguracyjny możliwy do edycji offline poza przełącznikiem wraz z możliwością przechowywania więcej niż jednego pliku konfiguracyjnego

Tak

Funkcjonalność PORT SPAN oraz RSPAN

Tak

Obsługa protokołów SNMPv3

Tak

Obsługa protokołów SSHv2

Tak

Zarządzanie za pomocą linii komend (CLI) poprzez SSH oraz port konsoli

Tak

Obsługa min. 4 poziomych dostępu administracyjnych przez konsolę zarządzania

Tak

Obsługa protokołu NTP lub SNTP

Tak

Obsługa protokołu 802.3ab LLDP i LLDP-MED. Lub równoważnych (np. CDP)

Tak

Obudowa przystosowana do montażu w szafie 19" wraz z osprzętem

Tak

Kabel zasilający – napięcie i rodzaj wtyku

Zmienne 230V, 50Hz, C13

Tabela 9 Parametry wymaganego przełącznika pod systemy bezpieczeństwa :

Porty i sloty	24 porty RJ-45 10/100/1000 POE+ z automatycznym wykrywaniem (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3at PoE+); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 SFP+ 1/10GbE ports; PHY-less
----------------------	--

Dodatkowe Porty i sloty	1 dual-personality (RJ-45 or USB micro-B) port konsoli
Waga	8.6 lb (3.90 kg)
Pamięć i procesor	Dual Core ARM Cortex @ 1016 MHz, 1 GB DDR3 SDRAM; Packet buffer size: 12.38 MB 4.5MB Ingress/7.875MB Egress, 4 GB eMMC
Wydajność	1000 Mb Latency < 3.8 μ s (64-byte packets) 10 Gbps Latency < 2.9 μ s (64-byte packets) Przepustowość: do 95.2 Mpps Przełączanie: 128 Gbps Rozmiar tablicy routingu: 2,000 IPv4, 1,000 IPv6 in hardware, 200 OSPF, 256 Static, 10,000 RIP Rozmiar tablicy adresów MAC: 32768 entries
Środowisko	Temperatura robocza: 0°C do 45°C; Wilgotność: 15% do 95% @ 40°C, bez kondensacji Temperatura przechowywania: -40°C do 70°C Poziom hałasu: Moc: 54,1 dB, Ciśnienie: 40,6 dB Wyrzut ciepłego powietrza: na boki Wydzielane ciepło: 258 BTU/hr (272,2 KJ/hr)
Elektryczność	Napięcie zasilania: 100 - 127 / 200 - 240 VAC Prąd: 4.9/2.4 A Maksymalna moc znamionowa: 445 W
Bezpieczeństwo	UL 60950-1, 2nd Edition; UL 62368-1: 2nd Edition; EN 60950-1:2006 +A11:2009 +A1:2010 +A12:2011+A2:2013; IEC 60950-1:2005 +A1:2009 +A2:2013; EN 62368-1: 2nd Edition; CSA 22.2 No. 60950-1-07 2nd; IEC-62368-1: 2nd Edition; EN 60825-

	1:2014 / IEC 60825-1:2014 Class 1
Emisyjność	EN 55032:2012/CISPR 32 Class A; FCC CFR 47 Part 15 Class A; VCCI Class A; ICES-003 Class A; CNS 13438
Odporność	Ogólne EN 55024: 2010 / CISPR 24 ESD IEC 61000-4-2 Promieniowane IEC 61000-4-3 EFT / Burst IEC 61000-4-4 Przepięcie IEC 61000-4-5 Porażenie IEC 61000-4-6 Pole magnetyczne o częstotliwości sieciowej IEC 61000-4-8 Spadki i przerwy napięcia IEC 61000-4-11 Harmoniczne IEC / EN 61000-3-2 Wahania napięcia IEC/EN 61000-3-3
Zarządzanie	Przełącznik zarządzalny min. na poziomie L2/L3 z obsługą VLAN 802.1q, ACL na poziomie L3/L4, routingu IP i min. 4 strefami bezpieczeństwa (VLAN)
Port security	Tak, dla poszczególnych portów
Trunking 802.1q	Tak
Obsługa RST (802.1w), PVRST	Tak
Obsługa MSTP (802.1s)	Tak
Obsługa IGMP snooping	Tak
Obsługa agregacji portów (802.3ad/LACP)	Tak
Obsługa ramek Jumbo	Tak, do min. 9216 bajtów
Funkcjonalność Strom control (unicast, multicast i broadcast)	Tak

Funkcjonalność PVLAN lub analogicznej (np. Port isolation)	Tak
Autoryzacja w oparciu o 802.1x z możliwością dynamicznego przypisania użytkownika do VLAN i ACL	Tak
Uwierzytelnienie urządzeń w oparciu o adres MAC	Tak
Funkcjonalność suplikanta 802.1x	Tak
Funkcjonalność Port security	Tak
Funkcjonalność DHCP Snooping	Tak
Funkcjonalność Dynamic ARP Inspection	Tak
Funkcjonalność IP Source Guard	Tak
Autoryzacja prób logowania do urządzenia na serwerach RADIUS lub TACACS+	Tak
Funkcjonalność STP Root guard	Tak
Funkcjonalność STP Port	Tak
Implementacja min. 4 kolejek dla ruchu wyjściowego na każdym porcie dla ruchu o różnej klasie oraz implementacja algorytmu Shaped Round Robin lub podobnego do obsługi tych kolejek oraz możliwość obsługi jednej z tych kolejek z bezwzględny priorytetem (Strict Priority)	Tak
Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie adresów MAC, IP lub portów TCP	Tak
Współpraca z serwerem Syslog	Tak
Liczniki pakietów wchodzących/wychodzących dla każdego portu	Tak
Tekstowy plik konfiguracyjny możliwy do edycji offline poza przełącznikiem wraz z możliwością przechowywania więcej niż jednego pliku konfiguracyjnego	Tak
Funkcjonalność PORT SPAN oraz RSPAN	Tak

Obsługa protokołów SNMPv3	Tak
Obsługa protokołów SSHv2	Tak
Zarządzanie za pomocą linii komend (CLI) poprzez SSH oraz port konsoli	Tak
Obsługa min. 4 poziomych dostępu administracyjnych przez konsolę zarządzania	Tak
Obsługa protokołu NTP lub SNTP	Tak
Obsługa protokołu 802.1ab LLDP i LLDP-MED. Lub równoważnych (np. CDP)	Tak
Obudowa przystosowana do montażu w szafie 19" wraz z osprzętem	Tak
Kabel zasilający – napięcie i rodzaj wtyku	Zmienne 230V, 50Hz, C13

Tabela 10 Dane techniczne wymaganego kabla połączeniowego do przełączników DAC:

Typ	Kabel połączeniowy typu DAC
Złącze	SFP+
Długość	1m

Tabela 11 Dane techniczne wymaganego kabla zasilającego do przełączników:

Typ	Kodowany kabel zasilający 10A/250V, 17AWG/1mm ² ,
Złącze zakończeniowe	IEC C14 na IEC C13
Długość	0,6m
Kolor	Czerwone
Kodowanie	Tak
Ośłona	SJT/H05VV-F

Dostarczane przełączniki i akcesoria muszą być zgodne z serią urządzeń posiadanych przez zamawiającego w sposób umożliwiający stworzenie stacka poprzez połączenia min. 10G za pomocą dedykowanych kabli połączeniowych typu DAC. Urządzenia muszą być zarządzane z poziomu tego

samego interfejsu co obecne przełączniki i nie mogą powodować konieczności zakupu czy posiadania dodatkowych platform zarządzających czy administracyjnych.

Dostarczone urządzenia muszą pochodzić z oficjalnego i autoryzowanego kanału sprzedaży producenta urządzenia na terenie Polski, a wykonawca musi zapewnić zamawiającemu możliwość weryfikacji numerów seryjnych dostarczonego sprzętu u producenta w celu sprawdzenia czy urządzenie pochodzi z legalnego kanału sprzedaży i czy nie jest zarejestrowane u producenta na innego klienta końcowego.

1.8 Administracja i dokumentacja

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, zarówno od strony gniazda PL, jak i od strony szafy montażowej. Te same oznaczenia należy umieścić w sposób trwały na gniazdach telekomunikacyjnych w obszarach roboczych oraz na panelach krosowych.

Konwencja oznaczeń okablowania poziomego:

X / Y/ C/

gdzie:

X – identyfikator szafy,

Y – numer panela krosowego,

C – numer portu w panelu.

Bezwzględnie wszelkie elementy wchodzące w skład systemu okablowania strukturalnego oraz sieci LAN muszą zostać trwale oznaczone w sposób umożliwiający jednoznaczną identyfikację zgodnie z ANSI/TIA-606-C.

Należy oznaczyć wszelkie:

- Kable,
- Kable krosowe,
- Panele krosowe,
- Racki,
- Gniazda logiczne,
- Urządzenia sieciowe.

1.9 Wymagania gwarancyjne

Gwarancja na system okablowania strukturalnego ma spełniać poniższe warunki:

- § gwarancja ma być jednolitą bezpłatną usługą serwisową świadczoną przez producenta okablowania (tj. bez ponoszenia jakichkolwiek kosztów w przyszłości związanych z przeglądami, serwisowaniem czy innymi pracami związanymi z naprawą i powtórna instalacją wadliwych elementów);
- § ma obejmować całość okablowania miedzianego, światłowodowego oraz telefonicznego wraz z kablami krosowymi i innymi elementami niezbędnymi do budowy sieci takimi jak panele krosowe, gniazda RJ45, adaptory światłowodowe, pigtaile, wieszaki, szafy itp.;
- § minimalny czas trwania 25 lat ma być udzielany na oficjalnych warunkach, ogólnie znanych i opublikowanych;
- § gwarancja ma być udzielona przez producenta okablowania bezpośrednio Inwestorowi/Użytkownikowi,
- § zastosować urządzenia klimatyzacji z minimum pięcioletnim okresem gwarancji,
- § zastosować UPSa (podtrzymanie gniazd i szaf) z minimum trzyletnim okresem gwarancji.

1.9.1 Obowiązki producenta okablowania

Producent systemu okablowania w swojej gwarancji systemowej ma zapewniać:

- § gwarancję materiałową (w przypadku wykrycia wady lub usterki fabrycznej, produkty wadliwe zostaną naprawione bądź wymienione);
- § gwarancję parametrów łącza/kanału (parametry łącza stałych bądź kanałów będą przewyższać wskazaną klasę okablowania w ciągu trwania całego okresu gwarancyjnego);
- § gwarancję aplikacji (protokoły sieciowe współczesne i stworzone w przyszłości, które zaprojektowane były lub będą dla systemów okablowania danej klasy będą działać poprawnie w ciągu całego okresu gwarancyjnego).

Instalacja ma być nadzorowana w trakcie budowy przez inżynierów ze strony producenta.

Zbudowana infrastruktura kablowa ma być ostatecznie fizycznie sprawdzona przez producenta przed wystawieniem certyfikatu gwarancyjnego pod kątem technicznym, funkcjonalnym oraz estetycznym. Użytkownik/Inwestor musi otrzymać raport, potwierdzający sprawdzenie instalacji oraz ma prawo uczestniczyć w procesie jej weryfikacji.

1.9.2 *Obowiązki instalatora*

W celu ujawnienia procedury, jak również zapoznania Użytkownika/Inwestora z prawami, obowiązkami i ograniczeniami gwarancji, wykonawca ma posiadać aktualną umowę zawartą bezpośrednio z producentem okablowania regulującą uprawnienia, procedury, warunki i tryb udzielenia gwarancji Użytkownikowi. Wykonawca przed rozpoczęciem prac związanych z zakresem okablowania strukturalnego ma dostarczyć Zamawiającemu potwierdzenie faktu rozpoczęcia budowy instalacji wystawione przez producenta.

Wykonawca ma posiadać dyplomy ukończenia kursów kwalifikacyjnych, przez zatrudnionych pracowników w zakresie:

- instalacji;
- pomiarów, nadzoru, wykrywania oraz eliminacji uszkodzeń;
- projektowania okablowania strukturalnego, zgodnie z normami międzynarodowymi oraz procedurami instalacyjnymi producenta okablowania;

W przypadku jeśli wykonawca na etapie oferty korzysta z uprawnień osób trzecich, dokumenty te muszą uczestniczyć w nadzorze zadania lub być na każde wezwanie na etapie realizacji.

Powyższe kursy mają znajdować się w oficjalnej ofercie producenta.

Dokumenty mają być przedstawione Zamawiającemu przed podpisaniem umowy.

Dostarczone elementy pasywne (kable miedziane i światłowodowe, panele krosowe, kable krosowe, panele telefoniczne, adaptory światłowodowe, pigtaile, szafy wraz z wyposażeniem) składające się na system okablowania strukturalnego muszą być oznaczone nazwą lub znakiem firmowym tego samego producenta okablowania i pochodzić z jednolitej oferty rynkowej, będącej kompletnym systemem w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania gwarancji w/w producenta.

1.10 **Wymogi regulacyjne CPR**

Instalacje wykonywane w Unii Europejskiej podlegają przepisom dotyczącym wyrobów budowlanych (CPR). Nowe europejskie rozporządzenie dotyczące m.in. kabli miedzianych i światłowodowych zatytułowane "Rozporządzenie w sprawie wyrobów budowlanych" (CPR) weszło w życie 1 lipca 2017 roku. Proponowany dostawca okablowania musi być zgodny a nowym rozporządzeniem.

Proponowany dostawca okablowania powinien klasyfikować swoje obecne europejskie portfolio kabli miedzianych i światłowodowych poziomych, wykorzystując zatwierdzone jednostki

notyfikowane i tym samym zapewniając zgodność z wymaganiami Rozporządzenia o Wyrobach Budowlanych (CPR).

Rozporządzenie stanowi, że kable miedziane i światłowodowe stosowane wewnątrz budynków produkowane od 1 lipca 2017 r. muszą posiadać oznaczenie CE na opakowaniu oraz deklarację właściwości użytkowych (DoP) łatwo dostępną dla użytkownika.

W przypadku produktów wymienionych w tym dokumencie CPR dotyczy kabli miedzianych i światłowodowych. CPR określa, jak kable reagują w warunkach pożaru (tj. właściwości spalania, takie jak przenoszenie ognia, wytwarzanie dymu, kwas i płonące krople itp.). Poziom wydajności kabli jest oznaczony przez tzw. Euroklasy. Euroklasy są hierarchiczne, co oznacza, że można stosować materiały o wyższym oznaczeniu we wszystkich parametrach. Różne kraje mają różne minimalne wymagania Euroklas.

CPR nie ma zastosowania do patchcordów lub zestawów, które nie są na stałe zainstalowane w budynku.

Ten projekt wymaga, aby kable komunikacyjne spełniały co najmniej Euroklasę Dca.

1.11 Odbiór i pomiary sieci

Przed przystąpieniem do wykonania pomiarów wykonawca ma obowiązek poinformować odpowiednie służby inwestora o planowanym terminie ich wykonania. Pomiary wykonanie bez zgody inwestora nie będą akceptowane.

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest spełnienie wszystkich poniższych warunków:

- § wykonanie instalacji w sposób prawidłowy, zgodny ze sztuką, wymaganiami i obowiązującymi normami oraz z zachowaniem estetyki prac;
- § wykonanie kompletu pomiarów;
- § opracowanie i przekazanie dokumentacji powykonawczej Inwestorowi;
- § uzyskanie gwarancji systemowej producenta okablowania.

Wykonawstwo pomiarów sieci miedzianej Klasy EA powinno być zgodne z normą IEC 61935-1. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

Należy użyć miernika dynamicznego (analizatora), który posiada analizy parametrów, według aktualnie obowiązujących norm. Sprzęt pomiarowy musi posiadać aktualną kalibrację/legalizację (tj. certyfikat potwierdzający dokładność jego wskazań, wydany przez serwis producenta).

Na raportach pomiarowych muszą się znaleźć informacje dotyczące ustawień sprzętu pomiarowego (norma, typ kabla itp.), nazwa mierzonego łącza oraz wyniki pomiarów wraz z zapasami w stosunku do limitów z norm. Każdy wynik musi być jednoznacznie opisany jako poprawny lub niepoprawny.

1.11.1 Pomiary okablowania miedzianego

- ☐ Analizator okablowania wykorzystany do pomiarów sieci miedzianej musi charakteryzować się przynajmniej V klasą dokładności dla Klasy EA wg IEC 61935-1 (proponowane urządzenia to np. FLUKE DSX5000 lub DSX8000).
 - ☐ Pomiary sieci miedzianej dla Klasy EA należy wykonać na zgodność z ISO/IEC11801 lub EN50173-1 zachowując następującą kolejność:
 - ☐ Łącze stałe (Permanent Link) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego,
 - ☐ Kable krosowe przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego,
 - ☐ Kanał (Channel) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego;
 - ☐ Pomiary sieci miedzianej należy wykonać na zgodność z ISO/IEC11801 lub EN50173-1 z rozszerzeniem parametrów o rezystancję nie zrównoważenia (dla 4PPoE):
 - ☐ Pomiary łączy wykorzystujących wtyki MPTL należy wykonać zgodnie z ANSI-TIA568.2-D dla Klasy EA wykorzystując odpowiednie adaptory pomiarowe specyfikowane przez producenta sprzętu pomiarowego dla danej klasy okablowania;
- § Protokół pomiarowy każdego toru transmisyjnego poziomego miedzianego ma zawierać:
- o mapę połączeń;
 - o długość połączeń i rezystancje par;
 - o rezystancję nie zrównoważenia
 - o opóźnienie propagacji oraz różnicę opóźnień propagacji;
 - o tłumienie;
 - o NEXT i PS NEXT w dwóch kierunkach;
 - o ACR-F i PS ACR-F w dwóch kierunkach;
 - o ACR-N i PS ACR-N w dwóch kierunkach;
 - o RL w dwóch kierunkach;
- § Na raporcie (sporządzonym oddzielnie dla każdego łącza) mają być widoczne: wynik pomiaru, identyfikacja łącza, wskazanie normy oraz informacja opisująca wielkość marginesu pracy (inaczej zapasu, tj. różnicy pomiędzy wymaganiem normy a pomiarem, zazwyczaj wyrażana w jednostkach odpowiednich dla każdej mierzonej wielkości);
- § Raport pomiarowy ma jednoznacznie informować o poprawności pomiaru (dobry/zły, pass/fail);

1.11.2 Zawartość dokumentacji powykonawczej

Po zakończeniu prac instalatorskich należy wykonać i przekazać Użytkownikowi końcowemu dokumentację powykonawczą, która ma zawierać:

- Raporty z pomiarów dynamicznych okablowania.
- Rzeczywiste trasy prowadzenia kabli.
- Rysunki z oznaczeniami poszczególnych szaf, paneli krosowych i portów.
- Lokalizację przebiegów przez ściany i podłogi.

1.12 Uwagi końcowe

Trasy prowadzenia okablowania poziomego należy skoordynować z istniejącymi i wykonywanymi instalacjami w budynku m.in. dedykowaną oraz ogólną instalacją elektryczną, instalacją centralnego ogrzewania, wody, kanalizacji, itp.. Jeżeli w trakcie realizacji nastąpią zmiany prowadzenia tras instalacji okablowania oraz lokalizacji Punktów Logicznych lub wystąpią konflikty z innymi instalacjami, należy ustalić poprawione rozprowadzenie tras kablowych w porozumieniu z Projektantem.

Należy uziemić zgodnie obowiązującymi przepisami wszystkie metalowe korytka, drabinki kablowe, szafy kablowe wraz z osprzętem oraz inne urządzenia sieciowe, które zgodnie z instrukcją ich montażu tego wymagają.

Wszystkie materiały wprowadzone do robót muszą być nowe, nieużywane, najnowszych aktualnych wzorów.

2 SYSTEM MONITORINGU WIZYJNEGO (CCTV)

2.1 Cel systemu monitoringu wizyjnego

Głównym celem systemu monitoringu wizyjnego jest nadzór mienia, zapewnienie możliwości podejmowania niezwłocznych działań prewencyjnych w przypadku sytuacji zagrożenia w obrębie monitorowanego obiektu, przeciwdziałanie przestępstwom, a także zapis i przechowywanie danych w celach dowodowych i udostępnienia ich uprawnionym podmiotom. System opracowany jest na podstawie wytycznych Inwestora uwzględniając zaplanowaną uniwersalność i funkcjonalność przy zastosowaniu nowoczesnych technologii przesyłania różnego rodzaju danych.

2.2 Podstawa opracowania projektu

Podstawą do opracowania projektu systemu dozoru wizyjnego CCTV są przede wszystkim wytyczne Inwestora w zakresie zgodności z obowiązującymi normami oraz funkcjonalności i wydajności systemu. Lista obowiązujących norm dotyczących systemu dozoru wizyjnego CCTV:

- PN-EN 50132-1:2012E – Systemy alarmowe – Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 1: Transmisja wideo – Wymagania systemowe.
- PN-EN 50132-5-1:2012E – Systemy alarmowe – Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 5-1: Transmisja wideo – Ogólne wymagania eksploatacyjne.
- PN-EN 50132-5-2:2012E - Systemy alarmowe – Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 5-2: Protokoły sieciowe (IP) dotyczące transmisji wideo;
- PN-EN 50132-5-3:2013-04E – Systemy alarmowe – Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 5-3: Transmisja wideo – Analogowa i cyfrowa transmisja wideo.
- PN-EN 50132-7:2013-04E – Systemy alarmowe – Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 7: Wytyczne stosowania.
- PN-EN 62676-1-1:2014-06 – Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne.
- PN-EN 62676-1-2:2014-06 – Systemy dozоровe CCTV stosowane w zabezpieczeniach Część 1-2: Wymagania systemowe – Wymagania eksploatacyjne dotyczące transmisji wizji.
- PN-EN 62676-2-1:2014-06 – Systemy dozоровe CCTV stosowane w zabezpieczeniach Część 2-1: Protokoły transmisji wizji – Wymagania ogólne.
- PN-EN 62676-2-2:2014-06 – Systemy dozоровe CCTV stosowane w zabezpieczeniach Część 2-2: Protokoły transmisji wizji – Zastosowanie międzyoperacyjności IP oparte na usługach HTTP i REST.
- PN-EN 62676-2-3:2014-06 – Systemy dozоровe CCTV stosowane w zabezpieczeniach Część 2-3: Protokoły transmisji wizji – Zastosowanie międzyoperacyjności IP oparte na usługach Web.
- PN-EN 62676-3:2015-06 – Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 3: Analogowe i cyfrowe interfejsy wizyjne.
- PN-EN 62676-3:2015-11 – Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 3: Analogowe i cyfrowe interfejsy wizyjne.
- PN-EN 62676-4:2015-06 – Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 4: Wytyczne stosowania.

Norma dotycząca projektowania instalacji ochrony odgromowej:

- PN-EN 50130-4:2012 – Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów. Wymagania dotyczące odporności urządzeń systemów sygnalizacji pożarowej, sygnalizacji włamania, sygnalizacji napadu, CCTV, kontroli dostępu i osobistych.

- PN-EN 62305-3:2011 – Ochrona odgromowa – Część 3: Uszkodzenia fizyczne obiektów i zagrożenie życia.

Uwaga: W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy.

2.3 Architektura i ogólny opis działania systemu monitoringu wizyjnego

2.3.1 Opis ogólny działania systemu

- Podgląd wejść, klatek schodowych oraz obszarów wewnątrz będzie realizowany za pomocą systemu monitoringu wizyjnego, przy użyciu cyfrowych, megapikselowych kamer działających w oparciu o protokół TCP/IP. Strumienie wideo z kamer mają być zapisywane na dyskach rejestratora sieciowego NVR (*ang. Network Video Recorder*).
- Zdarzenia jak i sama wizja ma być wyświetlana na monitorach zainstalowanych w pomieszczeniu 1.19.

2.3.2 Architektura systemu – obszary funkcjonalne

- Elementy końcowe – kamery IP kopułkowe o minimalnej rozdzielczości 3Mpix. Kamery o zmiennej ogniskowej posiadające wbudowany promiennik podczerwieni IR w budowie wandaloodpornej.
- Urządzenia rejestrujące – lokalne urządzenia rejestrujące materiał wideo znajdują się w pomieszczeniu serwerowni na 1 piętrze budynku – w szafie GPD.
- Sieć teletechniczna wraz z wyposażeniem sieciowym – urządzenia oraz media transmisyjne pozwalające na połączenie wszystkich elementów systemu monitoringu wizyjnego.
- Stacja operatorska systemu CCTV wyposażone w monitory o rozdzielczości min. Full HD, klawiaturę i mysz.

2.4 Wymagania ogólne dotyczące systemu monitoringu wizyjnego CCTV

Zgodnie z warunkami architektury oraz wymaganiami Użytkownika/Inwestora w zakresie bezpieczeństwa budynku, projektuje się system dozoru CCTV działający w oparciu o protokół internetowy IP (*ang. Internet Protocol*), który ma spełniać następujące funkcje oraz założenia uzgodnione z Użytkownikiem:

- Liczbę i rozmieszczenie elementów systemu dozoru wizyjnego CCTV przyjęto na podstawie informacji podanych przez Użytkownika.
- Projektowana budowa systemu monitoringu wizyjnego CCTV ma zawierać kamery działające w oparciu o protokół internetowy IP.
- Założono rejestrację nagrań z kamer w celu rozpoznania osób, identyfikacji danych osób oraz rejestracji zdarzeń.
- Wszystkie kamery wewnętrzne mają nagrywać w sposób ciągły.
- Zaprojektowano system działający w oparciu o sieć TCP/IP – rejestrator sieciowy NVR (*ang. Network Video Recorder*) zainstalowany w szafie GPD w serwerowni oraz kamery IP.
- Okablowanie do kamer oraz rejestratorów budowane jest w konfiguracji gwiazdy i przy rygorze, że łącza stałe nie mogą przekroczyć długości 90 m dla połączeń w oparciu o medium miedziane.
- Do wszystkich kamer kopułkowych ma zostać doprowadzony kabel podwójnie ekranowany S/FTP kat.7, 23 AWG w osłonie trudnopalnej LSFRZH (kabel opisany szczegółowo w dokumentacji okablowania strukturalnego);
- Zaprojektowano stację operatorską w pomieszczeniu 1.19 – do obsługi systemu dozoru wizyjnego CCTV oraz KD przez operatorów/ administratorów.
- System ma umożliwiać podłączenie różnych kamer produkowanych przez wielu producentów, obsługiwanych przez dedykowane oprogramowanie.
- System dozoru wizyjnego CCTV ma zapewniać pełną międzyoperacyjność w komunikacji między wieloma urządzeniami systemu różnych producentów.
- System ma zapewniać zdalny dostęp z dowolnego miejsca oraz urządzenia korzystającego z sieci za pomocą dedykowanych bezpłatnych wieloplatformowych aplikacji na urządzenia mobilne (iOS, Android).
- System ma mieć możliwość rozbudowy o rejestratory hybrydowe, tzn. podłączenie systemu CCTV analogowego wraz z systemem CCTV cyfrowym wykorzystującym protokół internetowy (IP) do transmisji obrazu oraz zapewniać ich płynne i szybkie działanie.
- System ma mieć funkcję automatycznego wykrywania podłączonych urządzeń systemu dozoru wizyjnego CCTV.
- Urządzenia rejestrujące obraz, tj. kamery mają mieć funkcję szerokiego zakresu dynamiki (WDR), pozwalającą na automatyczne dostosowanie obrazu do trudnych warunków oświetleniowych, zarówno ciemnych jak i jasnych, a także funkcję redukcji szumów.
- System ma mieć dodatkowo możliwość rozbudowy o integrację z systemami kontroli dostępu, sygnalizacji włamania i napadu, systemu detekcji pożaru oraz posiadać funkcje zaawansowanej analizy obrazu wideo pozwalającej na szybką reakcję na nietypowe zdarzenia, a także generowanie raportów oraz wykresów przedstawiających dane.

- Ma mieć możliwość tworzenia konkretnych zdarzeń w systemie dozoru wizyjnego CCTV oraz łączenia ich z innymi systemami bezpieczeństwa.
- Ma posiadać funkcję wtrącenia ważnego wydarzenia podczas obserwacji obrazu z wielu kamer w momencie pojawienia się nietypowego zachowania.
- Wydarzenia/alarmy/powiadomienia systemu dozoru wizyjnego CCTV mają być monitorowane z poziomu jednego oprogramowania.
- Przeszukiwanie nagranych zdarzeń ma odbywać się na podstawie nagrań ciągłych, a także szczególnych wydarzeń/ruchu w celu skrócenia czasu wyszukiwania.
- Oprogramowanie VMS klienckie musi być w pełni konfigurowalne aby dostosować go do wymagań każdego użytkownika.
- Do każdego użytkownika systemu musi być możliwość przypisania hasła dostępu oraz nadanie odpowiednich uprawnień.
- System powinien udostępniać dane na temat zajętości oraz wykorzystywaniu pamięci za pomocą danych statystycznych;
- System powinien posiadać opcje monitorowania stanu pamięci;
- System powinien udostępniać listę kamer, która można sortować i filtrować w celach organizacyjnych;
- System powinien pozwalać na konfigurowanie ustawień i funkcji kamer takich jak: edycja nazwy i opisu, zmiana adresu IP;
- System powinien umożliwiać konfigurację ustawień obrazu kamer w tym: rodzaj kompresji, liczbę klatek/s, rozdzielczość, ustawienie strumieniowania;
- System powinien umożliwiać tworzenie harmonogramów do zapisu wideo, do aktywowania wykrywania ruchu itp.
- System musi posiadać opcje automatycznego przeszukiwania sieci i wykrywania kamer.
- Sugeruje się szybkość zapisu na dysku rejestratora sieciowego co najmniej 15 kl/s, natomiast kamery mają posiadać szybkość rejestracji obrazu min. 30 kl/s.
- Rejestratory sieciowe mają mieć wbudowaną pamięć na nagrania o pojemności pozwalającej na przechowanie zapisu z kamer z okresu co najmniej 30 dni.
- Projektowane kamery wewnętrzne muszą być wyposażone w oświetlacz świecący falami podczerwieni (diody LED), zapewniający podgląd w nocy lub w słabych warunkach oświetleniowych na odległość co najmniej 40 metrów.
- Kamery muszą charakteryzować się klasą ochronności IP67 lub wyższą oraz być zabezpieczone przez ograniczniki przepięć.

- Wszystkie zaprojektowane kamery muszą posiadać stopień ochrony wandaloodporności co najmniej IK10.

2.5 Rozwiązania szczegółowe dotyczące systemu dozoru wizyjnego

System dozoru wizyjnego będzie składał się z dedykowanych urządzeń służących do transmisji oraz zapisu nagrań w odpowiedniej rozdzielczości i szybkości, tworzących spójną oraz wydajną infrastrukturę sieciową, zapewniającą bezpieczną komunikację między wszystkimi urządzeniami składowymi.

2.5.1 Urządzenia wymagane do realizacji systemu monitoringu wizyjnego CCTV

Rejestrator sieciowy NVR – obsługujący do 64 kanałów IP, dedykowany do ciągłej pracy. Rejestrator należy zainstalować w pomieszczeniu serwerowni – w szafie GPD.

Pamięć rejestratora ma umożliwiać zachowanie obrazu ze wszystkich kamer przez 30 dni pracujących przez całą dobę przy maksymalnej rozdzielczości kamer oraz płynności zapisu co najmniej 15 klatek na sekundę.

Rejestrator ma być urządzeniem specjalizowanym z odpowiednio zabezpieczonym systemem operacyjnym. Dodatkowo, dla dostępu administracyjnego do rejestratora ma być możliwość ustawienia hasła o długości co najmniej 12 znaków. Rejestrator ma posiadać kodeki MJPEG, H.264, H.265. Oprogramowanie rejestratora ma obsługiwać wiele modeli kamer różnych producentów.

Oprogramowanie rejestratora systemu dozoru wizyjnego CCTV ma być zainstalowane na dostarczonym sprzęcie spełniającym wymagania do jego uruchomienia i prawidłowego działania.

W celu obliczenia wymaganej ilości pamięci na nagrania wykorzystano specjalistyczny kalkulator pamięci uwzględniający szereg istotnych parametrów wpływających na zużycie pamięci. W tabeli 4.1 przedstawiono wyniki obliczeń przy uwzględnieniu wymienionych parametrów. Założono rodzaj zapisu nagrań w trybie ciągłym.

Tabela 12 Obliczenia potrzebnej ilości pamięci na nagrania – zapis co najmniej 30 dni w trybie ciągłym.

Opis	Liczba	Rozdzielczość	Kodek	FPS	h/dobę	Liczba dni	Przepustowość (Mbps)	Wymagana pamięć (TB)
Kamera kopułkowa	9	3M	H.264	15	24	30	2.36	6.88

Sumaryczna obliczona pamięć potrzebna do rejestracji wizji ze wszystkich kamer przez okres 30 dni wynosi 6.88 TB. W przypadku zaprojektowanego urządzenia rejestrującego – rejestrator sieciowy NVR – 8 TB, daje to 1,12 TB zapasu do wykorzystania w razie potrzeby.

Rejestrator sieciowy NVR – Obsługujący do 64 kanałów IP ma posiadać wbudowaną pamięć o pojemności co najmniej 8 TB, dzięki czemu zapewniony zostanie zapis nagrań na okres co najmniej 30 dni. Rejestrator ma zapewniać prędkość zapisu obrazu ze wszystkich kamer na poziomie co najmniej 450 Mb/s.

Tabela13 Minimalne wymagania dla rejestratora sieciowego NVR

Nazwa	Rejestrator systemu dozoru wizyjnego CCTV
Maksymalna liczba kamer IP	64
Pojemność dysku	8 TB
Kompresja	H.264 H.265
Zasilanie	100-240 VAC
Pobór mocy	160W Max, 110W Typowo
Sieć	2 x 1 GigE NiCs
Prędkość zapisu	450 Mb/s
System operacyjny	Linux Ubuntu, ver. min 20.04
Pamięć ram	Min. 8 Gb
Procesor	Intel Core i5
Osobny dysk na system operacyjny	Tak, min. 128 Gb SSD
Montaż	2U, na szynach w szafie rack
Wymiary	8.9 x 42.6 x 54.7 cm
Wyjścia obrazu	DVI-I, HDMI, DP, VGA, 2 Równocześnie
Gwarancja	Min. 3 lata sprzętowa oraz min. 3 lata aktualizacji oprogramowania w cenie urządzenia

Kamery IP wewnętrzne kopułkowe 3MP – mają posiadać rozdzielczości do 3 megapikseli ze zmienną ogniskową 3.2 – 10 mm. Kamera True Day/Night, która zapewnia rozdzielczość 3 MP dla wysokiej jakości obrazów w warunkach zewnętrznych. Obiektyw P-Iris zapewnia wyraźny obraz w zmieniającym się świetle. Ponadto kamera ma wbudowane oświetlacze podczerwieni, które zapewniają wyraźny obraz z efektywnej odległości w różnych warunkach słabego oświetlenia. Dodatkowo kamery mają posiadać możliwość konfiguracji przez aplikacje w smartfonie i WiFi. Kamery mają posiadać zaawansowane technologie umożliwiające otrzymanie wysokiej jakości obrazu: True WDR pozwalająca na automatyczne dostosowanie poziomu oświetlenia poszczególnych obszarów; kompresję wideo umożliwiającą rejestrację obrazu w rozdzielczości Full HD oraz szybkością do 60 klatek/s, nawet gdy występuje duży ruch oraz zmniejszenie szerokości pasma, gdy scena jest statyczna. Inteligentny promiennik podczerwieni IR umożliwiający płynne przełączenie pomiędzy rejestracją obrazu w dzień i w nocy; tryb True Day Night zapewniający wyraźne kolory w ciągu dnia jak i w nocy, obiektyw typu P-Iris umożliwiający ustawienie ostrości

dla całego obszaru obserwowanego przez kamerę. Kamery kopułkowe mają posiadać stopień ochrony min. IP67 oraz odporność na uderzenia min. IK10.

Kamery wewnętrzne mają zapewniać ciągły zapis danych przez 30 dni. Kamery mają spełniać wymagania podane w tabeli 4.4.

Tabela 14 Wymagania dla kamery IP kopułkowej 3Mpx

Nazwa	Kamera IP kopułkowa 3Mpx
Kompresja video	MJPEG, H.264, H.264 IntelliZip, H.265 and H.265 IntelliZip
Maks. częstotliwość klatek	H.265/H.264: Max. 60fps MJPEG: Max. 20fps
Rozdzielczość	2048x1536/ 1920x1080/ 1664x936/ 1280x720/ 1024x576/ 640x480/ 640x360/ 480x360/ 384x288
Strumień wideo	3
Przetwornik obrazu	1/2.8" 3.21MP CMOS
Rodzaj obiektywu	Zmotoryzowany obiektyw zmiennoogniskowy i ogniskowy, P-Iris
Długość ogniskowej	3.2 ~ 10mm
Pole widzenia	H: 94.7°(W)~29.34°(T) V: 68.7°(W)~22°(T) D: 125.21°(W)~36.45°(T)
Przesłona	f/1,6(W) f/2,9(T)
Minimalne oświetlenie	Kolor: min 0.05 lux (1/30sec, 30IRE) Czerń/Biel: 0.005Lux
Podświetlenie IR	40 m adaptacyjne
Zakres dynamiczny	True WDR 140 dB
Dzień/noc	Auto Niski/ Auto Średni (Domyślne)/ Auto Wysoki/ Ręczny/ Wymuszony Kolor/ Wymuś B&W
Efektywne piksele	2065(H) x 1553(V)
Zgodność z ONVIF 2.4	Profil S
Strefy wykrywania ruchu	3
Cyfrowa redukcja szumów	2D&3DNR
Wykrywanie rozmycia	Tak
Stosunek sygnału do szumu (SNR)	50db
Czas otwarcia migawki elektronicznej	Minimum 1/4s, Maximum 1/10,000s
Strefy prywatności	9
Tryby obrazu	Tryb korytarzowy, lustro i odwrócony
Alarmy wej/wyj	1/1
Micro USB	Obsługa konfiguracji Wi-Fi
Interfejs Ethernet	10/100 Ethernet, RJ-45
Kontrola szybkości transmisji	H.264/H.265: CBR or VBR or CVBR

Obsługiwane protokoły	TCP/IP, IPv4, IPv6, TCP, UDP, HTTP, FTP, DHCP, WS-Discovery, DNS, DDNS, RTP, RTCP, RTSP, TLS, Unicast, Multicast, NTP, ICMP, IGMP, SMTP, WS-Security, IEEE 802.1x, PEAP, EAP-TLS, EAPoL, SSH, HTTPS, SOAP, WSAddressing, CIFS, SNMP, UPNP, RTSP, LLDP
Bezpieczeństwo	Management, Multi-Level Password Protection, IP Address/ Filtering, HTTPS Encryption, One-Click Security Hardening, User Access Log, Validate Complex Credentials, Disabling Unused Protocols, IEEE / 802.1x Including: PEAP, EAP-TLS, EAPoL
Obsługa kart	Micro SD/SDHC/SDXC 1 slot 512GB
Wyzwalacz nagrywania	Wykrywanie ruchu, wykrywanie sabotażu, wejście alarmowe, wykrywanie rozmycia
Zdarzenia alarmowe	Wyjście alarmowe, nagrywanie na pokładzie, migawka, powiadomienie przez e-mail, przesyłanie FTP, przesyłanie CIFS
Zasilanie wejściowe	24 VAC (-20% ~ +30%, 47 ~ 63 Hz), PoE 802.3af (802.3at Type 1)
Pobór mocy	24 VAC: Max 12.6W PoE: Max 12.3W
Wymiary (prom. x wys.)	(Ø) 145 x (H) 106.5 mm
Waga	1 kg
Kolor obudowy	Biały sygnałowy - RAL 9003
Temperatura pracy	-40°C +50°C
Wilgotność	Do 90% bez kondensacji
Odporność na wandalizm	IK10
Klasa ochrony zewnętrznej	IP66/IP67
Bezpieczeństwo	UL62368-1; CAN/CSA-C22.2 No. 62368-1, BIS IS13252 Part 1:2010
Emisje	FCC Part 15 Class A; EN55032 Class A; AS/NZS CISPR 32 Class A; ICES-003/NMB-003 Class A
Odporność	EN50130-4
Środowisko	RoHS/WEEE, REACH

Stacja operatorska – dedykowana do obsługi systemu dozoru wizyjnego ma posiadać podzespoły spełniające wymagania do prawidłowego uruchomienia oraz działania oprogramowania klienckiego oraz możliwość podłączenia dziewięciu monitorów min 27” o rozdzielczości co najmniej Full HD. Oprogramowanie klienckie zainstalowane na stacji roboczej musi być jak najbardziej intuicyjne. Musi posiadać wbudowane narzędzia ułatwiające przeszukiwanie długich nagrań oraz predefiniowane układy dostępne dla operatora. Stacja operatorska ma obsługiwać wszystkie kamery w budynku. Zaprojektowano jedną stację operatorską dedykowaną dla obsługi systemu monitoringu wizyjnego CCTV.

Tabela 15 Minimalne wymagania komputera obsługującego monitoring CCTV

Procesor	Intel Core i9-10900X
Dysk	SSD 512 GB
Pamięć	16 GB DDR4
Max. wielkość pamięci	256 GB

Karta graficzna	NVIDIA Quadro P2000, 5 GB GDDR5
Karta sieciowa LAN	10/100/1000 Mbps
Napęd optyczny	DVD+/-RW 8x
Mini DisplayPort	10x
RJ-45	Tak
System operacyjny	Windows 10 Pro PL
Wymiary (szer. głęb. wys.)	177mm x 518mm x 418mm
Moc zasilacza	950 W

2.5.2 Montaż instalacji oraz prowadzenie okablowanie przeznaczonego dla systemu monitoringu wizyjnego CCTV

System monitoringu wykorzystuje kable okablowania strukturalnego – nowo projektowane kable S/FTP zgodne z projektem sieci LAN.

2.5.3 Montaż rejestratora sieciowego NVR

Rejestrator sieciowy NVR ma być zainstalowany w szafie GPD w pomieszczeniu serwerowni – w stelażu 19”.

2.5.4 Montaż urządzeń końcowych – kamer

Kamery IP kopułkowe 3MP– należy zamontować z wykorzystaniem dodatkowych puszek montażowych instalowanych pod kamerą, w celu przełączenia połączenia sieciowego z modułu RJ45 zakończonego na kablu instalacyjnym. Podłączenie samego urządzenia należy wykonać kablem krosowym umieszczonym wewnątrz puszek połączeniowej.

2.5.5 Zasilanie instalacji

Projekt systemu monitoringu wizyjnego CCTV zakłada zasilanie podstawowe wszystkich kamer IP poprzez kabel skrętkowy S/FTP kat. 7 , dzięki wykorzystaniu funkcji PoE/PoE+ dostępnych na portach przełącznika.

PoE/PoE+ dostępnych na portach przełącznika PoE lub rejestratora sieciowego.

2.5.6 Adminstracja

Sugerowana konwencja oznaczeń kamer:

KWX/Y/Z

gdzie:

K - kamera

W - typ kamery ("K" - kopułkowa, "T" - tubowa)

X - rodzaj kamery ("W" - wewnętrzna, "Z" - zewnętrzna)

Y - numer kamery

Z - lokalizacja montażu kamer ("-1" - piwnica, "0" - parter, "1" - I piętro, "2" - II piętro)

Po zakończeniu prac instalatorskich należy wykonać i przekazać Użytkownikowi końcowemu dokumentację powykonawczą, która ma zawierać:

- Raporty z pomiarów dynamicznych okablowania;
- Rzeczywiste trasy prowadzenia kabli;
- Rysunki z oznaczeniami poszczególnych szaf, paneli krosowych i portów;
- Lokalizację rzeczywistego rozmieszczenia kamer wraz z udokumentowaniem adresów MAC oraz adresów IP poszczególnych kamer.

3 SYSTEM KONTROLI DOSTĘPU (KD)

3.1 Cel systemu kontroli dostępu

Głównym celem systemu kontroli dostępu jest ograniczenie dostępu osobom nieupoważnionym do wyznaczonych pomieszczeń. Zaprojektowanie systemu opartego na powiązanych wzajemnie urządzeniach oraz zarządzanego poprzez specjalistyczne oprogramowanie ma pozwolić na nadawanie i odbieranie indywidualnych uprawnień do otwierania drzwi/dostawania się w określone miejsca. Wdrożenie umożliwi nadzór nad pracownikami, wywołanie alarmu w sytuacji naruszenia chronionego obszaru, zwiększenie bezpieczeństwa zasobów i mienia oraz uniemożliwienie dostępu osobom z zewnątrz.

3.2 Podstawa opracowania projektu

Podstawą do opracowania projektu systemu kontroli dostępu są wytyczne Inwestora w zakresie zgodności z obowiązującymi normami oraz funkcjonalności i wydajności systemu.

Lista norm wykorzystanych w projekcie:

- PN-EN 60839-11-2:2015-08 – wersja angielska - Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-2: Elektroniczne systemy kontroli dostępu – Wytyczne stosowania.

- PN-EN 60839-11-1:2014-01 – wersja angielska – Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i komponentów.
- PN-EN 60839-11-1:2014-01/Ap1:2019-06 – Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i komponentów.
- PN-EN 60839-11-1:2014-01/AC:2016-07 – Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i komponentów.
- PN-EN 60839-11-2:2015-08/AC:2015-12 – Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-2: Elektroniczne systemy kontroli dostępu – Wytyczne stosowania.

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

Uwaga: W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy.

3.3 Architektura systemu kontroli dostępu

3.3.1 Opis ogólny działania systemu

Za pomocą systemu kontroli dostępu ochroną zostaną objęte wybrane pomieszczenia w budynku. Dostęp do pomieszczeń będzie realizowany przy użyciu kontrolerów drzwiowych i czytników kart zbliżeniowych.

Wejście do pomieszczeń, ewentualne przejścia pomiędzy strefami będą realizowane za pomocą karty identyfikacyjnej poszczególnych osób mających dostęp (lub nie) do danego pomieszczenia/strefy. Każdorazowe wejście (przejście) zostanie zapisane jako zdarzenie w bazie danych systemu kontroli dostępu na serwerze.

Wszystkie kontrolery drzwi będą połączone w sieci Ethernet wykorzystując protokół TCP/IP do wzajemnej komunikacji. Programowanie przejść i uprawnień oraz odczytywanie danych z rejestru zdarzeń odbywać się będzie za pomocą oprogramowania zarządzającego.

Operatorzy systemu będą korzystać ze skonfigurowanej stacji operatorskiej systemu kontroli dostępu (KD). Wszelkie powiadomienia, alarmy oraz raporty będą wyświetlane na zainstalowanym monitorze KD.

3.3.2 Obszary funkcjonalne

W budynku zaprojektowano system kontroli dostępu w postaci:

- Kontroli wejścia, składającej się z trzech jednostronnie kontrolowanych drzwi z czujnikiem położenia drzwi oraz awaryjnym przyciskiem ewakuacyjnym po stronie wewnętrznej. Lista pomieszczeń/przejsć objętych kontrolą dostępu:

Parter:

- o Pom. 1.7,
- o Pom. 1.19,

1 Piętro:

- o Pom. 2.10,

Elementami składowymi system kontroli dostępu są:

- Serwer systemu kontroli dostępu z bazą danych.
- Stacja robocza z zainstalowanym oprogramowaniem klienckim.
- Czytniki z wbudowanym kontrolerem kontroli dostępu, działające w oparciu o protokół internetowy IP,
- Akcesoria drzwi (elektrozamek, kontaktron, przycisk wyjścia/wyjścia awaryjnego).
- Urządzenia zasilające (zasilacz 12 V DC oraz akumulator 7 Ah montowany w obudowie).

3.4 Wymagania ogólne dotyczące systemu kontroli dostępu

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

- Liczbę i rozmieszczenie elementów systemu kontroli dostępu przyjęto na podstawie założeń projektowych. System zaprojektowano z myślą o maksymalnym bezpieczeństwie.
- Okablowanie do kontrolerów drzwi budowane jest zgodnie z normami wymienionymi w dokumentacji projektowej okablowania strukturalnego, tj. w konfiguracji gwiazdy i przy rygorze, że łącza stałe nie mogą przekroczyć długości 90 m dla połączeń w oparciu o medium miedziane.
- Okablowanie przeznaczone dla systemu kontroli dostępu rozprowadzane do kontrolerów /czytników ma być obsługiwane przez szafę GPD w serwerowni.

- Do wszystkich kontrolerów i terminali ma zostać doprowadzony kabel ekranowany S/FTP kat.7 w osłonie zewnętrznej typu LSFRZH, trudnopalnej i niewydzielającej trujących substancji w obecności ognia (kabel opisany szczegółowo w dokumentacji projektowej okablowania strukturalnego).
- Kontrola dostępu ma być jednostronna (montaż czytnika kontroli dostępu po stronie zewnętrznej drzwi).
- System ma posiadać budowę modułową oraz działać on-line jak i offline.
- System ma posiadać architekturę klient – serwer.
- Kontroler ma być łączony w sieci poprzez Ethernet.
- Kontroler oraz osprzęt drzwiowy ma być zasilany poprzez dedykowany zasilacz 12V DC.
- Każdy kontroler ma posiadać podtrzymanie bateryjne (akumulatory 7 Ah) przy braku zasilania.
- Kontroler ma posiadać własną pamięć i pracować nawet bez połączenia z serwerem.
- System ma umożliwiać integrację z systemami SSWiN.
- System ma umożliwiać integrację z systemami sygnalizacji pożaru SSP.
- System ma umożliwiać integrację z systemem monitoringu wizyjnego CCTV,
- Oprogramowanie systemu ma być dostępne zarówno w wersji dedykowanego serwera z preinstalowanym systemem kontroli dostępu jak i w wersji do instalacji na innym sprzęcie spełniającym minimalne wymagania do jego uruchomienia w zależności do potrzeb użytkownika.
- Wersja oprogramowania ma być łatwo rozszerzalna wraz ze zwiększeniem się potrzeb użytkownika.
- System ma umożliwiać obsługę czytników biometrycznych.
- System ma mieć możliwość podłączenia czytników posiadających funkcję domofonu.
- System ma umożliwiać podział kontrolowanego obszaru na strefy i monitorowanie każdej z nich osobno.
- System ma udostępniać aplikację Web.
- System ma posiadać funkcję wizualizacji obiektu za pomocą map.
- System ma posiadać funkcję zdalnego otwierania drzwi.
- System musi posiadać funkcję obsługi kart zbliżeniowych.

- System kontroli dostępu ma mieć możliwość programowego łączenia zdarzeń z różnych systemów oraz alarmowania o nich za pomocą przeznaczonej do tego aplikacji.
- System musi posiadać wbudowany moduł oprogramowania integrującego SMS (Security Management System pozwalającego na integrację zainstalowanych w obiekcie systemów SSP, CCTV, KD, SSWIN.

3.5 Specyfikacja techniczna elementów składowych systemu kontroli dostępu

3.5.1 System kontroli dostępu

Głównym punktem obsługi systemu kontroli dostępu jest serwer (na którym ma być zainstalowana również baza danych systemu kontroli dostępu) z zainstalowanym oprogramowaniem, zaprojektowany do działania w architekturze klient – serwer. Oprogramowanie ma być dostarczane w dwóch wersjach: jedna dla stacji operatorskiej, druga dla wirtualnego serwera, który ma być zainstalowany i skonfigurowany w wirtualnym środowisku (Virtual Machine, VM). Oracle VM VirtualBox jako aplikacja na systemie operacyjnym stacji roboczej II – Microsoft Windows 10 Pro.

Oprogramowanie ma wykorzystywać zaawansowane rozwiązania sprzętowe, obejmujące czytniki kart inteligentnych i kontrolery obsługujące Ethernet, zapewniające również kompatybilność z czytnikami innych producentów. System ma wykorzystywać rozwiązanie oparte na rozproszonej inteligencji na wszystkich poziomach systemu, w tym czytników kart posiadających własną bazę danych, co dodatkowo zwiększa ogólną odporność systemu. Obsługa systemu ma następować z dedykowanej stacji operatorskiej z zainstalowanym oprogramowaniem klienckim.

System ma oferować pakiet aplikacji klienckich i przeglądarkowych, takich jak monitorowanie alarmów, tworzenie zaawansowanych identyfikatorów, zarządzanie gośćmi, raporty internetowe, integracja z systemami wielu producentów.

3.5.2 Serwer systemu

Zaprojektowano serwer dedykowany dla systemu kontroli dostępu KD. Zamontowany on będzie w szafie GPD znajdującej się w pomieszczeniu serwerowni, pomieszczenie 2.10 na 1 piętrze budynku. Minimalne wymagania serwera przedstawione są w tabeli 1.

Tabela 16 Minimalne wymagania dotyczące serwera

Procesor	min. Intel Core i5
Rozmiar	1U Rackmount
Zasilacz	350W High-efficiency Power Supply 80 PLUS, Gold Level Certified
Wentylatory	2x 4cm 4-pin PWM Fans
Kieszenie na dyski	2x 3.5" Internal Drive Bays

Rozmiar	microATX 9.6" x 9.6" (24.38cm x 24.38cm)
Obsługiwane procesory	8th Generation Intel Core i3/Pentium/Celeron Processor, Intel Xeon Processor E-2100 series.
Gniazdo procesora	Single Socket LGA 1151 supported
Porty usb	• 6 USB 2.0 ports (2 rear + 4 headers) • 5 USB 3.1 Gen1 ports (2 Rears Type A, 2 headers, 1 Type A)
Procesor	CFL-S 4C E-2224 3.4G 8M 71W 8GT/s DMI
Pamięć	8GB DDR4-2666Mhz 1Rx8 ECC UDIMM,HF,RoHS
Karta sieciowa	2xRJ45 1Gb/s Intel I350
Dysk twardy	Samsung PM883 480GB SATA 6Gb/s V4 TLC 2.5"
Oprogramowanie	Windows 10 Professional (64-bit)
Gwarancja	36 miesięcy door-to-door standard

3.5.3 Stacja operatorska

Zaprojektowano stację operatorską dla obsługi systemu kontroli dostępu KD oraz CCTV (punkt 4.5.1). Stacja ma posiadać podzespoły spełniające wymagania systemowe do prawidłowego uruchomienia i działania oprogramowania klienckiego oraz możliwości podłączenia monitorów 27". Zainstalowane oprogramowanie klienckie musi być jak najbardziej intuicyjne. Musi posiadać wbudowane narzędzia ułatwiające przeszukiwanie różnego rodzaju zdarzeń oraz predefiniowane układy dostępne dla operatora. Oprogramowanie musi również posiadać możliwość wyświetlania zdarzeń w sposób przejrzysty dla operatora oraz mieć możliwość wizualizacji urządzeń oraz ich statusu na interaktywnych mapach.

Kluczowe funkcje oraz aplikacje dostępne w oprogramowaniu klienckim:

- Identyfikatory VIPPS.
- Zarządzanie gośćmi.
- Wyświetlanie zdarzeń alarmowych.
- Obchody strażników.
- Ciągłe wyświetlanie transakcji.
- Monitor stref.
- Strefy przebywania ludzi.
- Rozszerzone raporty.
- Czas i obecność.
- Konfigurowanie komunikatów czytnika.

- Strefy zbiórki.
- Poziomy zagrożień.
- Standard System Link (Standardowe Łącze Systemowe).
- Szereg interfejsów nadzoru wideo.
- Aplikacje dla sieci WEB.
- Interfejsy paneli alarmowych.
- W pełni zintegrowane rozwiązania biometryczne.
- Integracja z Microsoft Active Directory.

3.5.4 Terminal/Kontroler drzwi z wbudowanym czytnikiem.

Zastosowany w projekcie system oferuje elastyczną i skalowalną platformę sprzętową. Oznacza to, że każde urządzenie może być skonfigurowane tak, aby spełniać konkretne potrzeby instalacji. W projekcie wykorzystano kontrolery z wbudowanym czytnikiem, wyposażone w kolorowy i czytelny wyświetlacz pozwalający w prosty i czytelny sposób identyfikować zdarzenia w systemie KD, obsługujące 3 przejścia (3 czytniki – kontrola jednostronna. Wszystkie urządzenia podłączone są w sieci Ethernet. Zaprojektowane kontrolery z czytnikami posiadają wbudowane na płycie łącze Ethernet i komunikują się bezpośrednio z systemem centralnym, bazą danych zainstalowaną na serwerze. Kontroler oferuje pełną zdolność walidacji (offline) i podejmowania decyzji w punkcie wejścia, gdy komunikacja z serwerem nie jest dostępna. Kontrolery z wbudowanym czytnikiem mają być zasilane poprzez zasilacz 12 V DC zainstalowany w obudowie zainstalowanej po stronie chronionej każdego przejścia. Kontroler ma mieć podtrzymanie z akumulatora 12 V DC 7 Ah montowanego również w obudowie zasilacza.

3.5.5 Terminal z wyświetlaczem dotykowym i wbudowanym czytnikiem

Najważniejsze cechy terminala:

- Ekran dotykowy LCD o przekątnej 4,3”.
- Intuicyjny interfejs graficzny użytkownika.
- Wykrywanie obecności dzięki czujnikowi PIR.
- Informacje konserwacyjne/inteligentny punkt ochrony.
- Wykrywanie ruchu PIR (sterowanie jasnością ekranu).

- Czytnik i kontroler Ethernet w jednym urządzeniu.
- Narzędzie do zdalnego programowania umożliwiające pobieranie nowego oprogramowania.
- Cztery wejścia analogowe do monitorowania stanów alarmowych oraz dwa wyjścia przekaźników do aktywowania rygla zamka drzwi i/lub innych urządzeń.
- Baza danych offline mieszcząca do 250 000 rekordów posiadaczy kart oraz do 50 000 transakcji offline.
- Obsługa szerokiej gamy technologii inteligentnych kart.
- Zasilanie z zasilacza lub PoE/PoE+
- Możliwość zastosowania wewnętrznego i zewnętrznego.

Specyfikacja techniczna

Terminal z wyświetlaczem dotykowym i wbudowanym czytnikiem zaprojektowany przy drzwiach wejściowych do pomieszczenia serwerowni. Zasilanie terminala będzie zapewnione za pomocą zasilacza zewnętrznego zainstalowanego po stronie chronionej pomieszczenia oraz wyposażonego w podtrzymanie za akumulatora. Do kontrolera doprowadzony będzie kabel krosowy z gniazda RJ45 umieszczonego w obudowie zasilacza, o parametrach przewidzianych w dokumentacji projektowej okablowania strukturalnego. W tabeli 5.3 przedstawiono minimalne wymagania dla terminala.

Tabela 17 Specyfikacja techniczna terminala

Parametry fizyczne	
Wymiary	157x108 x49 mm
Waga kontrolera	< 450 g
Obudowa	Ognioodporny poliwęglan zawierający całkowicie zamknięty w środku układ elektroniczny, kolor czarny
Wyświetlacz LCD	Pojemnościowy, dotykowy o przekątnej 4,3", 480*272 piksele, kolorowym, 16-bitowym
Zasilanie	
Napięcie	10-14 V DC
Pobór prądu	350 mA (typowo), 500 mA (max) – zasilanie PoE (brak możliwości zasilania elementów peryferyjnych – np. elektrozamka) 350 mA (typowo), 500 mA (max) – zasilanie PoE+ (850 mA dostępnych dla urządzeń peryferyjnych – np. elektrozamka)
Środowiskowe	
Temperatura pracy	-20° to 70°C – PoE

	-25° to 55°C – PoE+
Stopień ochrony IP	IP65
Funkcjonalność	
Wyjścia	2 przekaźniki, styki beznapięciowe
Wejścia dodatkowe	Cztery wejścia, sabotaż
Pamięć	128 MB RAM, 256MB NAND Flash
Obsługiwane technologie kart	MiFARE (CSN)/ DESFire (CSN)/ CEM DESFire/ iCLASS/ iCLASS SE
Bateria zapasowa RTC	3,0V akumulator litowo-jonowy
Pamięć użytkowników	do 250 000 użytkowników w trybie offline
Pamięć zdarzeń	do 50 000 operacji w trybie offline
Interfejsy komunikacyjne	
Czytniki	RS485, połączenia za pomocą zacisków śrubowych
Serwer	10/100BaseT TCP/IP kat.5 UTP, RJ45
Tryby pracy	Tryb drzwi, Śluza, Tryb przed drzwiowy, Globalny PIN, PIN jako karta
Interkom	SIP, VoIP, VOX 2-drożny half-duplex lub Push-to-Talk (konfigurowalne), kodek audio G.711, Tryb listy kontrolnej wpisów
Regulacje	FCC Part 15, CE, UL 294

Od strony wewnętrznej należy zainstalować przycisk wyjścia, który będzie umożliwił wyjście z pomieszczenia oraz przycisk wyjścia ewakuacyjnego.

Drzwi do pomieszczenia serwerowni należy wyposażać w elektrozaczep rewersyjny zasilany napięciem 12VDC oraz kontaktron pozwalający na nadzór otwarcia drzwi.

Drzwi od strony zewnętrznej jak i wewnętrznej należy wyposażać w pochwyt.

3.5.6 Terminal z wbudowanym czytnikiem kart i klawiaturą

W projekcie wykorzystano kontroler z wbudowanym czytnikiem kart, klawiaturą oraz wyświetlaczem LCD 2,4". Posiada możliwość połączenia w sieci Ethernet. Posiada możliwość komunikacji z czytnikami innych firm. Posiada wbudowane na płycie łącze Ethernet i komunikuje się bezpośrednio z systemem centralnym. Kontroler oferuje pełną zdolność walidacji off-line i podejmowania decyzji w punkcie wejścia, gdy komunikacja z komputerem głównym nie jest dostępna. Kontroler obsługuje czytniki kontroli dostępu innych firm zgodne z interfejsami fizycznymi Wiegand/RS485, obejmującymi szereg technologii począwszy od technologii zbliżeniowej RF aż do urządzeń biometrycznych. Kontroler z wbudowanym czytnikiem oraz osprzęt drzwiowy ma być zasilany z dedykowanego zasilacza. Kontroler ma mieć podtrzymanie zasilania przypadku braku napięcia sieciowego.

Najważniejsze cechy terminala

- Zintegrowany kontroler z czytnikiem IP
- Ekran LCD
- Klawiatura pojemnościowa do weryfikacji kodu PIN
- Prezentacja karty zbliżeniowej z możliwością włączenia numeru identyfikacyjnego pracownika (PIN) do uwierzytelniania dwuetapowego
- Kontekstowe klawisze funkcyjne do wyboru i nawigacji
- Graficzny wyświetlacz LCD o przekątnej 2,4'', do wyświetlania komunikatów
- Wysoki poziom bezpieczeństwa
- Możliwość wgrywania logo firmy i reklam
- Wyjście do obsługi czytnika dodatkowego Wiegand
- Obsługa czytników firm trzecich
- Obsługa jednego przejścia - dwustronna
- Strukturalna baza danych umożliwia przechowywanie dużych ilości zapisów posiadaczy kart w celu walidacji karty w trybie offline
- Cztery wejścia analogowe do monitorowania drzwi lub warunków alarmowych
- Dwa wyjścia przekaźnikowe
- Klasa odporności na wandalizm IK06 oraz odporność na kurz i wodę IP65

Tabela 18 Specyfikacja techniczna terminala.

Parametry fizyczne	
Wymiary	144 x 100 x 49 mm
Waga kontrolera	< 300 g
Obudowa	Ognioodporny poliwęglan zawierający całkowicie zamknięty w środku układ elektroniczny, kolor czarny
Wyświetlacz LCD	Pojemnościowy, dotykowy o przekątnej 2,4'', 240*320 piksele
Klawiatura	Tak, pojemnościowa
Zasilanie	
Napięcie	9-28 V DC
Środowiskowe	
Temperatura pracy	-20° do 60°C

Wilgotność	Max. 95%
Stopień ochrony IP	IP65
Wandaloodporność	IK06
Funkcjonalność	
Przełączalne wyjścia	2x 24V 2A
Wyjścia	2 przekaźniki, styki beznapięciowe
Wejścia dodatkowe	Cztery wejścia analogowe
Interfejs do podłączenia czytnika wewn.	Wiegand, RS-485
Pamięć	32 MB SDRAM Data: 2 Gb flash
Obsługiwane technologie kart	MiFARE (CSN)/ DESFire (CSN)/ CEM DESFire/ iCLASS/ iCLASS SE
Pamięć użytkowników	do 250 000 użytkowników
Pamięć zdarzeń	do 50 000 operacji
Interfejsy komunikacyjne	
Serwer	10/100BaseT TCP/IP, RJ45
Regulacje	FCC Part 15, CE

Od strony wewnętrznej należy zainstalować przycisk wyjścia, który będzie umożliwił wyjście z pomieszczenia oraz przycisk wyjścia ewakuacyjnego.

Drzwi do pomieszczenia 1.7 i 1.19 należy wyposażać w elektrozaczep rewersyjny zasilany napięciem 12VDC oraz kontaktron pozwalający na nadzór otwarcia drzwi.

Drzwi od strony zewnętrznej jak i wewnętrznej należy wyposażać w pochwyt.

3.5.7 Enkoder

Enkoder (czytnik USB służący do wczytywania kart do systemu):

- Czytnik musi być wyposażony w kabel ze złączem USB,

- Czytnik musi umożliwiać wyświetlenie/wpisanie, odczytanego nr karty na ekranie komputera w polu edycyjnym
 - Czytnik musi posiadać możliwość konfiguracji/wyboru z jakiego sektora, aplikacji, nr karty będzie czytany
 - Czytnik musi posiadać możliwość konfiguracji kluczy kryptograficznych służących do odczytu nr a kart/breloków/tagów kontroli dostępu
 - Czytnik musi pozwalać na odczytanie i wyświetlenie na ekranie komputera nr karty wirtualnej zgodnie z posiadaną konfiguracją
- (pozostałe parametry jak powyżej)**

3.5.8 Karty zbliżeniowe

W projekcie zastosowano programowalne karty zbliżeniowe z możliwością odczytu i zapisu danych na karcie. Karty posiadają interfejs bezdotykowy o częstotliwości 13,56 MHz. Wykonane są z wysokiej jakości materiału PCV, który pozwala na nadruk wszelkiego rodzaju dodatkowych informacji – zdjęć, numerów, itp.

Dzięki wykorzystaniu szyfrowania AES-128 informacje na karcie pozostają bezpieczne, co gwarantuje, że karta nie zostanie sklonowana i że dostęp umożliwiać będą ważne karty.

Podstawowe informacje:

- częstotliwość działania 13,56 MHz, odczyt/zapis;
- technologia kart Desfire EV2
- zaawansowane szyfrowanie AES-128 pomiędzy kartą a czytnikiem;
- max. bufor komunikacyjny 128 bajtów;
- krotność zapisu – min. 500 000 cykli;
- pamięć EEPROM, odczyt/zapis – w projekcie zastosowano 4kB;
- typowa odległość odczytu – do 10 cm;
- przechowywanie danych przez 25 lat.

3.5.9 Urządzenia dodatkowe

Do urządzeń dodatkowych systemu kontroli dostępu zaliczamy urządzenia obsługujące drzwi: elektrozamek, czujnik położenia (kontaktron), przycisk wyjścia oraz przycisk ewakuacyjny.

W projekcie wyspecyfikowano wymagania prądowo – napięciowe jakie muszą spełniać elektrozamki podłączane do kontrolerów kontroli dostępu. Należy zastosować elektrozamki rewersyjne na prąd stały. Podane napięcie – zapadka zamknięta, zdjęte napięcie zapadka otwarta.

Minimalne parametry techniczne jakie musi spełniać elektrozamek przedstawiono w tabeli 5.4.

Tabela 19 Minimalne wymagania dla elektrozamka

Napięcie	12 V DC
Tolerancja napięcia zasilania	10 – 14 V AC/DC
Typ	Rewersyjny
Siła trzymania	Min. 350 kg

Zastosowane w projekcie zasilacz znajduje się w zamykanej na klucz, metalowej obudowie, w której pozostawiono wolne miejsce na akumulator awaryjny. Zasilacz zapewnia zasilanie wszystkich urządzeń peryferyjnych podłączonych do kontrolera.

Tabela 20 Minimalne wymagania dla zasilacza

Zasilanie	200÷240VAC
Wyjście zasilania	3A/13.8VDC
Prąd ładowania akumulatora	0.5A
Akumulator	1 x 7Ah
Sprawność	87%
Wymiary	200 x 230 x 82 [+/-2 mm]
Zabezpieczenia	dystans od podłoża: 8 mm
Zamykanie	SCP, OLP, OVP, UVP, tamper – otwarcie obudowy
Montaż	skręcana (możliwość montażu zamka)
Sygnalizacja	natynkowy
Wykonanie	sygnalizacja optyczna LED
Stopień szczelności	blacha DC01, 0.7mm, RAL9003 (biały), metalowa
	IP 20

3.6 Montaż instalacji oraz prowadzenie okablowania

Ze względu na to iż budynek Ratusza podlega ochronie konserwatorskiej trasy okablowania należy wykonać zgodnie z zaleceniami Opolskiego Wojewódzkiego Konserwatora Zabytków, a także w sposób, który ma zapewniać łatwe, bezkolizyjne i bezpieczne prowadzenie kabli uwzględniając inne instalacje w budynku. Okablowanie należy prowadzić w następujący sposób:

- Przewody instalacyjne prowadzić podtynkowo;
- Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym, bez domieszek cementu oraz pomalować w kolorystyce analogicznej do istniejącej;
- Wskazane jest prowadzenie tras kablowych w części przypodłogowej ścian;\
- Nie dopuszcza się prowadzenia linii kablowych w obrębie zachowanych w budynku sklepień kolebkowych;

Terminale/kontrolery należy podłączyć do sieci komputerowej przez port RJ45 znajdujący w kontrolerach w celu administracji. Okablowanie do terminali zostanie rozprowadzone w pomieszczeniach kablem ekranowanym S/FTP kat.7 do punktu logicznego PL opisanego szczegółowo w projekcie okablowania strukturalnego i znajdującego się w obudowie zasilacza dedykowanego do obsługi każdego przejścia. Z modułu RJ45 umieszczonego w obudowie zasilacza należy poprowadzić kabel krosowy zgodnie ze specyfikacją opisaną w części dotyczącej okablowania strukturalnego sieci LAN, a następnie wpiąć go w port ethernetowy terminalu/kontrolera zgodnie z podkładami oraz schematami ideowymi. Czytniki będą posiadać możliwość autoryzacji uprawnionego użytkownika za pomocą karty zbliżeniowej.

Jako wejścia, za pomocą kabli YTDY 2x0,5 mm należy połączyć kontaktron do monitorowania stanu otwarcia/zamknięcia drzwi, oraz przycisk wyjścia służący do otwarcia chronionego przejścia od strony wewnętrznej pomieszczenia. Dodatkowo do terminala/kontrolera należy połączyć jako wyjście elektrozamek za pomocą kabla OMY 2x1,5mm połączony przez odpowiednie styki awaryjnego przycisku wyjścia.

Należy pamiętać o maksymalnych długościach kabli do poszczególnych elementów systemu i należy ich bezwzględnie przestrzegać:

- Połączenie RS485 (czytnik – kontroler) – 1200 m (zalecane nie przekraczać 1000 m);
- Połączenie Wiegand (czytnik – kontroler) – 150 m (zalecane nie przekraczać 100 m);
- Połączenie kontaktron – kontroler – 600 m;
- Połączenie zasilanie – kontroler – 8 m;
- Połączenie elektrozamek – kontroler – długość zależna od mocy elektrozamka i przekroju kabla.

3.7 Zasilanie instalacji

Zasilanie podstawowe:

- Przewiduje się zastosowanie zasilaczy 12 V DC.
- Przewiduje się zastosowanie akumulatora kwasowo – ołowiowego 12 V DC, 7 Ah zamontowanego w metalowej obudowie wraz z zasilaczem jako opcja zasilania awaryjnego dla terminala/kontrolera.

3.8 Odbiór instalacji systemu kontroli dostępu

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest spełnienie wszystkich poniższych warunków:

- Wykonanie instalacji w sposób prawidłowy, zgodny ze sztuką, wymaganiami i obowiązującymi normami oraz z zachowaniem estetyki prac.
- Wykonanie kompletu pomiarów.
- Uruchomienie oraz skonfigurowanie wszystkich urządzeń systemu kontroli dostępu KD (tj. serwera oraz stacji operatorskiej, kontrolerów, czytników).
- Opracowanie i przekazanie dokumentacji powykonawczej Inwestorowi.

System kontroli dostępu oparty jest na instalacji okablowania strukturalnego. Należy stosować się do wytycznych zawartych w odpowiedniej dokumentacji.

3.9 Uwagi dotyczące prowadzenia okablowania

Trasy prowadzenia okablowania należy skoordynować z wykonywanymi instalacjami w budynku, czyli ogólną instalacją elektryczną oraz innymi branżami. Jeżeli w trakcie realizacji nastąpią zmiany prowadzenia tras instalacji okablowania oraz lokalizacji punktów instalacji urządzeń końcowych (kontrolerów lub czytników) lub wystąpią konflikty z innymi instalacjami, należy ustalić poprawione rozprowadzenie tras kablowych oraz wszelkie inne zmiany w porozumieniu z Projektantem. Zgodnie z obowiązującymi przepisami, należy uziemić wszystkie metalowe części, obudowy kontrolerów, szafy dystrybucyjne wraz z osprzętem oraz inne urządzenia sieciowe, które zgodnie z instrukcją ich montażu tego wymagają.

Wszystkie materiały wprowadzone do robót muszą być nowe, nieużywane oraz najnowszych aktualnych wzorów.

4 System Sygnalizacji Włamania i Napadu (SSWiN)

4.1 Część ogólna

Przedmiotem niniejszego opracowania jest dokumentacja projektowa instalacji Systemu Sygnalizacji Włamania i Napadu oraz dedykowanego zasilania. Niniejsza dokumentacja dotyczy budowy infrastruktury teletechnicznej i elektrycznej. Dokumentację opracowano na podstawie planów i zapotrzebowania Inwestora, wg. wytycznych i zaleceń, uwzględniając zaplanowaną uniwersalność i

funkcjonalność przy zastosowaniu zintegrowanych nowoczesnych technologii przesyłania różnego rodzaju danych

4.1.1 Podstawa opracowania

Podstawę do opracowania niniejszego projektu stanowią:

- Ustawą z dnia 7 lipca 1994r. Prawo budowlane, (t.j. Dz.U. z 2006r. nr 156 poz. 1118 z późniejszymi zmianami).
- Rozporządzeniem Ministra Infrastruktury z dnia 12 kwietnia 2002r. w sprawie warunków technicznych jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. z 2002r. nr 75 poz. 690 z późniejszymi zmianami).
- Informacje producentów urządzeń systemów SSWiN.
- PN-76/E-05125 Elektroenergetyczne i sygnalizacyjne linie kablowe. Projektowanie i budowa. PN-90/E-05023 Oznaczenia identyfikacyjne przewodów barwami lub cytrami.
- PN-EN 60529:2003 Stopnie ochrony zapewniane przez obudowy (Kod IP);
- Polskie Normy „Systemy alarmowe” PN-93/E-08390 (wszystkie arkusze, bez arkusza 13).
- PN-EN 50131-1:2002 Systemy alarmowe- Systemy sygnalizacji włamania - Część 1: Wymagania ogólne;
- PN-EN 50131-6:2002 Systemy alarmowe - Systemy sygnalizacji włamania - Część 6: Zasilacze;
- PN-EN 50130-4: 1995 Kompatybilność elektromagnetyczna.

4.2 Opis systemu

Zaprojektowany system spełnia ostre wymagania stawiane przy zabezpieczaniu obiektów o średniej skali wielkości. Podstawową częścią systemu jest jednostka centralna, która decyduje o jego możliwościach sprzętowych i programowych. Jednostka centralna posiada 2 magistrale transmisyjne RS485, do których dołączane są moduły systemu obsługujące 264 linie z możliwością rozbudowy do max 520 lini. Dzięki przyjętemu sposobowi komunikacji poszczególne moduły systemu mogą być oddalone od centrali do 1,2 km.

System SWiN zaprojektowano zgodnie ze stopniem Grade 2 (PN-EN 50131). Charakterystyka stopnia 2 oznacza ryzyko małe do średniego. Dla tego stopnia wymaga się, aby system wykrywał otwarcie drzwi, okien i innych zamknięć chronionego obszaru oraz wykrywał poruszanie się w chronionym obszarze (pułapkowo). Zaprojektowane urządzenia: min. Stopień II, klasa

środowiskowa min. II, jednak ze względu na zaawansowanie techniczne urządzeń, w ramach niniejszego projektu należy przyjąć dla wszystkich elementów **min. stopień Grade 3**.

System posiada otwartą architekturę sprzętową i programową, co pozwala na rozwijanie systemu w miarę zmieniających się potrzeb użytkownika bez konieczności wymiany całego sprzętu. System posiada funkcję samokonfiguracji i automatyczne rozpoznanie modułów przyłączonych do magistrali RS485 oraz przyjęcie tzw. standardowych parametrów po włączeniu urządzenia do sieci zasilającej.

Centrala jest wyposażona w dodatkowy moduł rejestru zdarzeń A033. Pozwala on na dodatkowe zarejestrowanie 150 000 zdarzeń. W rozległym systemie włamaniowym generowane są bardzo duże ilości zdarzeń systemowych każdego dnia. Moduł zapewnia długi czas rejestrowania tych zdarzeń w sprzętowej nieulotnej pamięci, co pozwoli uniknąć nadpisania istotnych z punktu widzenia bezpieczeństwa czy zaistniałych sytuacji alarmowych zdarzeń systemowych.

Funkcje linii dozorowych oraz wyjść wykonawczych są realizowane w systemie przez podcentrale (ekspandery – koncentratory). Każda podcentrala posiada 8 linii dozorowych parametryzowanych oraz 4 wyjścia programowalne (wersja z zasilaczem lub bez). System dysponuje funkcjami diagnostycznymi. Jedną z opcji systemu jest możliwość pomiaru rezystancji linii dozorowej, napięcia na wyjściach zasilających poszczególne moduły systemu oraz pomiar poboru prądu z poszczególnych zasilaczy typu SMART PSU. Istotną zaletą systemu jest funkcja wykonywania programowych połączeń, służących do wzajemnego powiązania linii dozorowych, wyjść programowalnych, kodów klawiatur itp.

Każda linia dozorowa musi obsługiwać elementy w standardzie 3EOL i 4 EOL oraz prezentować co najmniej 8 stanów linii dozorowej tj.: alarm normalny, awaria, sabotaż zwarcie, sabotaż rozwarcie, wysoka rezystancja, niska rezystancja.

Zadaniem Systemu Sygnalizacji Włamania i Napadu jest ochrona obiektu, poprzez powiadomienie służb ochrony wewnętrznymi i zewnętrznymi sygnalizatorami alarmu oraz wywołanie stanu alarmu na stacji wizualizacyjnej (operatorskiej) w systemie zarządzającym obiektem. Wszystkie moduły systemu SSWiN zostaną zamontowane w obudowach zabezpieczonych przed sabotażem otwarcia oraz oderwania do ściany.

Obsługa systemu możliwa będzie z:

- poziomu klawiatury LCD;
- z poziomu dedykowanej aplikacji producenta np. WIN-PAK.

Sygnały alarmowe powinny zostać zaprogramowane w taki sposób, aby jednoznacznie można było określić rodzaj zdarzenia np.: włamanie, napad, sabotaż oraz miejsce jego wystąpienia. Wszystkie zdarzenia będą gromadzone w pamięci centrali, module rejestru zdarzeń ora będą wysyłane do stacji zarządzającej (operatorskiej). Zdarzenie SSWiN będą wizualizowane na stanowisku komputerowym na rzutach obiektu z naniesionymi elementami Systemu Sygnalizacji Włamania i Napadu.

4.3 Okablowanie i trasy kablowe

Ze względu na to iż budynek Ratusza podlega ochronie konserwatorskiej trasy okablowania należy wykonać zgodnie z zaleceniami Opolskiego Wojewódzkiego Konserwatora Zabytków, a także w sposób, który ma zapewniać łatwe, bezkolizyjne i bezpieczne prowadzenie kabli uwzględniając inne instalacje w budynku. Okablowanie należy prowadzić w następujący sposób:

- Przewody instalacyjne prowadzić podtynkowo;
- Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym, bez domieszek cementu oraz pomalować w kolorystyce analogicznej do istniejącej;
- Wskazane jest prowadzenie tras kablowych w części przypodłogowej ścian;
- Nie dopuszcza się prowadzenia linii kablowych w obrębie zachowanych w budynku sklepień kolebkowych;

Dla instalacji SSWiN wykonać okablowanie zgodnie z wymaganiami producenta zabudowanych urządzeń.

Zasilacze modułów rozszerzeń zasilane powinny być z obwodów elektrycznych. Obwody zasilające należy zabezpieczyć wyłącznikami instalacyjnymi.

Przewody teletechniczne powinny być prowadzone wyłącznie w bezpiecznej odległości od przewodów silnoprądowych oraz tablic rozdzielczych wynoszącej przynajmniej 50 cm lub z wykurzaniem odpowiednich przegród separujących od instalacji silnoprądowych. Czujek nie należy montować w bezpośrednim sąsiedztwie tablic rozdzielczych, innych urządzeń elektrycznych wydzielających silne pole elektromagnetyczne oraz w miejscach w których występuje możliwość zakłócenia ich pracy, np. nie montować czujek skierowanych w stronę okien zewnętrznych.

Zastosowane przewody:

- CAB4/TP/75 2x2x0,75 mm² firmy CQR Security – magistrala RS485;
- CABS6 6x0,22 – połączenie czujek i przycisków, sygnalizatorów;
- OMY 2x1,5 – kabel zasilający elektrozaczepy, zwory;
- YDYżo 3x2,5 – zasilanie centrali i podcentral.

Uwagi montażowe:

- montaż wszystkich elementów systemu zgodnie z wytycznymi producenta;

- centralę wyposażać w moduł sieciowy oraz dobrany akumulator zamontowany w obudowie;
- unikać zbliżeń oraz krzyżowań instalacji niskoprądowej z silnoprądową.

4.4 Zasilanie

Zasilanie dla centrali i podcentral będzie wykonane z najbliższej rozdzielni elektrycznej za pomocą dedykowanego obwodu przewodem YDYżo 3x2,5. Cały system będzie zasilany awaryjnie z akumulatorów 12V/18Ah (centrala i podcentrala). Zastosowana pojemność akumulatorów zapewni pracę systemu SSWiN przez minimum 60 godzin w stanie czuwania + 30 minut w stanie alarmu.

4.5 Wymagania dotyczące sprzętu

Centrala minimalnie 48 linii:

- min. 1000 użytkowników oraz obsługa min. 48 linii dozorowych;
- obsługa 8 niezależnych grup, podsystemów;
- dodatkowy rejestr zdarzeń do 150 000 wpisów;
- obsługa 2 akumulatorów 18 Ah/12 V;
- interfejs wielojęzyczny (ang, pol);
- kontrola dostępu 4 czytniki zbliżeniowe z możliwością rozbudowy do 8 czytników;
- 1 magistrale systemowe pracujące w standardzie RS485 9600bit/s, transmisja half duplex, asynchroniczna;
- obsługa min. 1 klawiatury dotykowej TOUCH CENTER;
- współpraca z systemowymi urządzeniami bezprzewodowymi za pośrednictwem specjalizowanego modułu RF 868 MHz;
- interfejs RS232 56k wbudowany na płytę;
- moduł telekomunikacyjny do monitorowania systemu w standardzie SIA, DTMF, MICROTECH, CONTACT ID wbudowany na płytę;
- możliwość współpracy centrali z siecią LAN/WAN za pośrednictwem interfejsu ETHERNET z wykorzystaniem protokołów TCP/IP/UDP wraz z szyfrowaniem

transmisji oraz możliwością programowania modułu zapasowego w celu uzyskania toru transmisji rezerwowej;

- możliwość współpracy z modułem ISDN – 2B+D;
- obsługa dedykowanego klucza SPI dla archiwizacji konfiguracji centrali;
- możliwość przejścia z magistralą na światłowody przy użyciu standardowego konwertera np. produkcji MOXA TCF-142;
- możliwość wizualizacji oraz sieciowania central przy użyciu protokołu komunikacyjnego;
- możliwość weryfikacji alarmów wbudowanym torem audio;
- wbudowany nadzorowany zasilacz typ A o wydajności min. 3A w tym 1,5A dla akumulatora. Nadzorowane stany (prąd pobierany z zasilacza, napięcie, akumulator, sieć 230 V, bezpieczniki – wszystkie stany muszą być dostępne z poziomu dowolnego manipulatora LCD podpiętego do systemu);
- wyjścia zasilania 2 kpl. 12 V/1 A – poziom tętnień <50 mV;
- pobór prądu centrali 150 mA;
- obsługa linii dozorowych pracujących w standardzie 3EOL oraz 4EOL – w celu bezpośredniej obsługi antymaskingu oraz wyjść diagnostycznych podpinanych do systemu urządzeń;
- temperatura pracy od –10 do +55 stopni;
- Norma PD6662: 2003 Schemat zastosowań norm europejskich dla Systemów Sygnalizacji Włamania;
- Norma EN50131-1:2003 Systemy alarmowe – Systemy włamaniowe. Wymagania ogólne (stopień 3);
- Norma TS50131-3 Systemy Alarmowe – Systemy włamaniowe: Część 3 – Urządzenia sterujące i wskazujące (stopień 3);
- Norma EN50131-6: 1998 Systemy Alarmowe – Systemy Włamaniowe – Zasilacze (stopień 3);
- Norma EN50136 – 1 – 1: 1998r Systemy Alarmowe – Systemy Transmisji Alarmów – Wymagania ogólne dla systemów transmisji alarmów;

- Norma EN50136 – 1 – 3: 1998r Systemy Alarmowe – Systemy Transmisji Alarmów – Wymagania dla systemów wykorzystujących cyfrowe moduły komunikacyjne pracujące w publicznej sieci telefonicznej;
- CE;
- R&TTE 99/5/EC;
- BS 6799:1996.

Moduł dodatkowego rejestru zdarzeń (150 000 tys.):

- pojemność w wersji podstawowej: ok. 150 000 zdarzeń;
- możliwość rozbudowy do max. 800 000 zdarzeń;
- programowanie i serwisowanie za pomocą interfejsu TCP/IP;
- oprogramowanie z bazą SQL w zestawie;
- integracja z centralą poprzez interfejs RS232 lub moduł drukarkowy A161;
- różne poziomy dostępu (serwis/operator/administrator);
- zastosowanie: obiekty infrastruktury kluczowej, rozległe systemy kontroli dostępu, systemy z dużą ilością linii dozorowych oraz sterowań;
- zastępuje standardową drukarkę analogową w systemach z pełnym zarządzaniem w środowisku IP;

Moduł Ethernet:

- | | |
|-------------------------------------|-----------------------|
| - interfejs komunikacyjny fizyczny: | TCP/IP (złącze RJ-45) |
| - obsługiwane protokoły: | TCP/IDP; UDP |
| - prędkość komunikacji: | 100Base-T / 10Base-T |
| - szyfrowanie transmisji: | TAK 128 bit |
| - napięcie zasilania: | 12–15 V |
| - pobór prądu: | 110 mA |
| - obsługa protokołu SIA: | TAK poziomy 0–4 |

- zgodność: PD6662:2004/2010, EN50131-1:2006
Grade 4, Environmental Class II, ATS Class 6

Koncentrator z zasilaczem Grade 3

Dane techniczne z podłączonym akumulatorem 34 Ah z zachowaniem postanowień normy EN50131 poziom 3:

- napięcie wejściowe: 230 V a.c. (+10% / -15%), 50Hz
- napięcie wyjściowe (nominalnie): 13,8 V oraz 14,5V
- prąd wyjściowy (max): 3,0A
- temperatura pracy: -10 st. C do +40 st. C
- napięcie wyjściowe (nominalne) AUX1: 13,8 V
- napięcie wyjściowe (nominalne) AUX2: 13,8 V
- prąd wyjściowy (max): 0,75 A z każdego wyjścia
- napięcie wyjściowe (nominalne) AUX 14,5V: 14,5 V
- prąd wyjściowy (max): 0,15 A (prąd wyjściowy z AUX1 oraz AUX2 zostanie proporcjonalnie zredukowany, gdy będzie używany to wyjście)
- prąd ładowania akumulatora (max): 1,4 A
- poziom tętnień: < 100mV
- test akumulatora: raz na 1 godzinę i przy każdym wyjściu z trybu inżyniera.
- obecność akumulatora: test on-line
- odcięcie akumulatora: automatyczne poniżej 10 V
- maksymalna pojemność akumulatora: 34 Ah
- miejsce na akumulator: 1x28 Ah lub 2x18 Ah z modułem A079 kontroli

- bezpiecznik F1 14,5 V: 500 mA, 20 mm zwłoczny,
nadzorowany przez system
- bezpiecznik F2 Akumulator: 1,6 A, 20 mm zwłoczny
nadzorowany przez system
- bezpiecznik F3 12V AUX1: 1 A, 20 mm zwłoczny, nadzorowany przez
system
- bezpiecznik F4 12V AUX2: 1 A, 20 mm zwłoczny, nadzorowany przez
system
- bezpieczniki F1,F2,F3,F4: Nadzorowane przez system ich stan
dostępny z poziomu manipulatora
- EN50131- 6 Zasilacze: Poziom 3
- PD6662:2004: TAK
- klasa środowiskowa: II
- typ zasilacza: A
- pobór prądu: 100 mA
- wymiary obudowy: 420x310x85 mm
- materiał obudowy: Stal, kolor popielaty
- sabotaż obudowy (zdjęcie pokrywy): TAK niezależne wejście
- sabotaż obudowy (oderwanie od podłoża): TAK niezależne wejście
- linie dozorowe: 8 szt. 2EOL lub 3EOL lub 4EOL
- wyjścia programowalne: 4 szt. OC 400 mA każde
- wyjścia OC diagnostyki wewnętrznej: FAULT OP AC – uszkodzenie
AC FAULT OP BAT – uszkodzenie
akumulatora
OP POWER – niskie nap.
AUX FAULT
na wyj.
- praca autonomiczna: TAK tryb SLAVE lub E/E

- pomiary z poziomu manipulatora: Prąd AUX 1 oraz AUX2
- napięcie na akumulatorze: Prąd ładowania akumulatora

Stan bezpieczników
 Poziom komunikacji z CA
 Test akumulatora
 Czas podtrzymania
 Czas ładowania po usterce napięcie na module

Manipulator systemowy (Grade 3, z klapką)

- napięcie wejściowe: 10,5-16 VDC
- zgodność z EN50131: Stopień 3
- klasa środowiskowa: II
- pobór prądu: 70 mA
- wymiary obudowy: 149 x 91 x 31 mm
- rodzaj materiału: ABS, kolor biały
- waga : 213g
- wyświetlacz: 2x16 znaków
- sabotaż oderwania od podłoża: TAK
- sabotaż zdjęcia obudowy: TAK
- pomiary z poziomu manipulatora: Poziom komunikacji z
CA Napięcie na module
- regulacja głośności: TAK
- wbudowany auto-test: TAK
- optyczna sygnalizacja stany zasilania systemu: TAK

Czujka ruchu PIR z antymaskingiem z wbudowanymi rezystorami

- typ detekcji: PIR (optyka lustrzana)
- zasięg: 16 x 22 m

- rezystory EOL: Alarm&sabotaż: 1K, 2.2K, 4.7K & 5.6K; fabr.=1K
Antymasking: 2.2K, 3K; fabr.=3K
- strefy detekcji: 36 daleki zasięg, 10 średni, 12 mały, 2 str. podejścia
- test chodzony: 20 s
- odporność na RFI: 15 V/m, 80 MHz – 2.7 GHz
- wysokość montażu: Zalecana 2.3 m
- zasilanie: 9 – 15 VDC
- pobór prądu: 11 mA maksymalnie
- przek. alarmu: Typ A / 30 mA@25 VDC, max 22 Ohm / Czas: 3s
- przek. antymaskingu: Typ B / 30 mA@25 VDC, max 22 Ohm
- przek. sabotażu: Typ A / 30 mA@25 VDC – Pokrywa & od ściany
- temperatura pracy: -10°C do +55°C
- kompensacja temp.: Dualna
- wilgotność pracy: 5% - 95% bez kondensacji
- odporność na RF: 30 V/m od 10 MHz do 1000 MHz
- odporność światło białe: 10 000 LUX
- wymiary: 116 x 70 x 43 mm (Wy.xSz.xGł)
- waga: 118 g
- certyfikaty zgodności: EN50131-2-2 Grade 3 Class II. NF&A2P 3 shields, Insert, IMQ,

Kontaktron wpuszczany z wbudowanymi rezystorami

- podłączenie: 4 zaciski
- szczelina: 16 mm zamknięcie, 5 sabotaż (drewno)
- rodzaj magnesu: Alnico 5

- wymiary: 36x9
- typ styku: Normalnie zamknięty (NC)
- zakres napięć: 1-48 V DC
- polaryzacja : TAK
- maksymalny obciążenie styku: 500 mA@12 VDC
- tamper: obudowa + RFMS
- zgodny z normą EN50131-2-6: stopień 3,
- klasa środowiskowa: 3

4.6 Przeglądy okresowe

W celu zapewnienia ciągłego poprawnego funkcjonowania instalacji, ma ona być regularnie sprawdzana i poddawana okresowym przeglądom. Umowy na ten temat powinny być zawarte pomiędzy użytkownikiem, a organizacją serwisową natychmiast po zakończeniu instalowania.

Obsługa codzienna:

Należy zapewnić, aby w każdy dzień roboczy wykonane było następujące sprawdzenie, polegające na stwierdzeniu, że:

- Centrala wykazuje stan normalnej, bezusterkowej pracy, a każda odchylenie od stanu normalnego jest zapisywane w książce eksploatacji i jest przekazywane do odpowiedniej organizacji prowadzącej obsługę techniczną.
- Każdy alarm zarejestrowany od poprzedniego dnia roboczego został należycie potraktowany.
- Instalacja została odpowiednio przywrócona do stanu podstawowego po każdym wyjściu ze stanu normalnej pracy.

Każde zauważone uszkodzenie powinno być zapisane w książce eksploatacji, a działania naprawcze powinny być podjęte tak szybko, jak to jest możliwe.

Obsługa miesięczna:

Co najmniej raz w miesiącu użytkownik musi zagwarantować, aby:

- Wykonano kontrolę i testy rutynowe zalecane dla obsługi codziennej.

- Wykonany był test wskaźników i zgłoszono ewentualne uszkodzenie jakiegokolwiek wskaźnika.

Każde uszkodzenie powinno być zapisane w książce eksploatacji i akcja naprawcza powinna być podjęta tak szybko, jak to jest możliwe.

Obsługa kwartalna:

Co najmniej jeden raz na 3 miesiące użytkownik ma zagwarantować, aby kompetentna osoba (serwisant):

- przeprowadziła kontrolę i testy rutynowe zalecane dla obsługi codziennej, miesięcznej;
- sprawdziła wszystkie wpisy do książki eksploatacji i podjęła wszelkie niezbędne działania, ażeby doprowadzić do prawidłowej pracy instalacji;
- spowodowała zadziałanie czujek w celu sprawdzenia zdolności centrali do odbioru i wyświetlenia poprawnego sygnału alarmu, do emisji alarmu dźwiękowego oraz do uruchomienia wszelkich innych urządzeń pomocniczych;
- sprawdziła funkcje nadzorowania uszkodzeń centrali;
- tam, gdzie jest to dopuszczalne, spowodowała zadziałanie każdego łącza do stacji monitorującej lub do zdalnego centrum z obsługą;
- zbadała, czy zaistniały jakiekolwiek zmiany budowlane lub zasiedleniowe, które mogą wpłynąć na wymagania dotyczące rozmieszczenia czujek i sygnalizatorów dźwiękowych.

Każde uszkodzenie powinno być zapisane w książce eksploatacji, a działania naprawcze powinny być podjęte tak szybko, jak to jest możliwe.

Obsługa roczna:

Co najmniej raz do roku użytkownik musi zagwarantować, aby kompetentna osoba (serwisant):

- przeprowadziła kontrolę i testy rutynowe zalecane dla obsługi codziennej, miesięcznej i kwartalnej; sprawdziła każdą czujkę pod względem poprawności działania, zgodnie z zaleceniami producenta; sprawdziła zdolność centrali do wykonywania wszelkich pomocniczych funkcji;
- wykonała sprawdzenie przez oględziny w celu potwierdzenia, że wszystkie połączenia kablowe i aparatura są pewne, nieuszkodzone i odpowiednio zabezpieczone;
- wykonała kontrolę wzrokową w celu sprawdzenia, czy zmiany budowlane, lub w zasiedleniu zakłóciły zasady dotyczące rozmieszczenia przycisków napadowych, czujek i sygnalizatorów dźwiękowych. Kontrola wzrokowa powinna również potwierdzić, że przed każdą czujką jest

zapewniona wolna przestrzeń we wszystkich kierunkach oraz że wszystkie elementy obsługowe i przyciski pozostają dostępne;

- zbadała wszystkie baterie zasilania rezerwowego.

Każda bateria powinna być wymieniana w odstępach czasu nie przekraczających zaleceń podanych przez producenta baterii.

Każde zauważone uszkodzenie powinno być zapisane w książce eksploatacji, a działania zapobiegawcze powinny być podjęte tak szybko, jak to jest możliwe.

Należy zwrócić uwagę, ażeby wszystkie urządzenia zostały po kontroli przywrócone do normalnego stanu pracy.

4.7 Zasilanie systemu alarmowego

Zasilanie AC 230 V

Urządzenia systemu zainstalowane w budynku mają być zasilane z obwodu rozdzielnic elektrycznej zgodnie z rzutami instalacji załączonymi do projektu.

Zasilanie DC 12 V

Zasilanie awaryjne DC 12 V, ma być realizowane w oparciu o zasilacz centrali alarmowej oraz obudów z modułami obsługi zasilacza z akumulatorami o dobranej pojemności 18 Ah. Dostarczają one zasilanie awaryjnego systemu alarmowego w przypadku braku podstawowego zasilania z sieci 230 V AC. Zgodnie PN-EN 50131-1 Systemy alarmowe przyjęto maksymalny czas pracy systemu na zasilaniu awaryjnym wynoszący 60 godzin.

5 System sygnalizacji pożarowej SSP

5.1 Podstawa opracowania

- ☐ Zlecenie Inwestora
- ☐ Obowiązujące normy i przepisy w zakresie opracowania.
- ☐ Umowa zawarta z Inwestorem
- ☐ Wytyczne branżowe
- ☐ Zlecenie Inwestora
- ☐ Wytyczne techniczne wydane przez Inwestora
- ☐ Ustawa prawo budowlane z dn. 07.07.94 r (Dz.U. 2017r. poz.1332)

- ☐ Ustawa o ochronie przeciwpożarowej z 24 sierpnia 1991r Nr 81 poz. 351 (Dz.U. z 2020r poz. 961, 1610) z późniejszymi zmianami
- ☐ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7.06.2010 w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. Nr 109 poz. 719).
- ☐ Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. Nr 75 poz. 690 z 2002 r.)
- ☐ PN-E-08350-14 Systemy sygnalizacji pożarowej
- ☐ PKN-CEN / TS 54-14: 2006 Normy Unijne
- ☐ Podręcznik projektanta systemów sygnalizacji pożarowej – CNBOP 2006 r.
- ☐ Wstęp do automatycznych systemów sygnalizacji pożarowej – CNBOP – 1996 r.

5.2 Zakres opracowania

- ☐ Opis systemu sygnalizacji pożaru
- ☐ Karty katalogowe, instrukcje obsługi urządzeń
- ☐ Certyfikaty urządzeń
- ☐ Koncepcja prowadzenia instalacji
- ☐ Trasy kablowe
- ☐ Lokalizacja urządzeń
- ☐ Schemat blokowy systemu

5.3 Charakterystyka obiektu

Budynek ratusza jest obiektem wolnostojącym z wieżą ratuszową, wybudowany w latach 1550-1552. Pierwotnie budowla składała się z dwóch prostokątnych budynków, zakończonych trójkątnymi zdobionymi szczytami. Z boku przystawiono wieżę, w dolnej części kwadratową, wyżej przechodzącą w ośmiobok. W latach 1821–1822 budowla została gruntownie przebudowana, w wyniku czego została jej nadana obecna neoklasycystyczna forma. W okresie 1911-1912 wykonano dekoracje stiukową w sali posiedzeń rady miejskiej. W latach późniejszych budynek został przebudowany i rozbudowany. Budynek ratusza został wybudowany z cegły i kamienia. Budynek posiada piwnicę, trzy kondygnacje nadziemne oraz strych. Obecny budynek ratusza pochodzi z pierwszej połowy XIX wieku i w obecnym czasie pełni siedzibę Urzędu Miasta w Paczkowie. Na pierwszym piętrze budynku znajduje się sala sesyjna o wysokości dwóch kondygnacji budynku, sklepiona kolebką o łuku koszowym. Wszystkie pomieszczenia budynku są użytkowane jako pomieszczenia biurowe, a na strychu budynku znajduje się wydzielona część pomieszczenia o charakterze archiwalno-magazynowym. Renesansowa wieża wysokości 45 m usytuowana jest w północnym narożniku budowli. Do wejścia prowadzą dwubiegunowe schody. Podstawa wieży ma przekrój kwadratowy, znajdują się w niej pomieszczenia ze sklepieniami kolebkowym. Wyższa część ma przekrój ośmioboczny, na narożach są wałki, tworzące rzędy półkolistych wnęk arkadowych. Wieża udostępniona jest do zwiedzania dla turystów.

5.4 Założenia podstawowe

Przedmiotem niniejszego opracowania jest dokumentacja projektowa instalacji Systemu Sygnalizacji Pożaru. Niniejsza dokumentacja dotyczy budowy infrastruktury systemu wczesnego wykrywania pożaru wraz z dedykowanym zasilaniem z sieci elektrycznej. Dokumentację opracowano na podstawie planów i zapotrzebowania Inwestora, wg. wytycznych i zaleceń, uwzględniając zaplanowaną uniwersalność i funkcjonalność przy zastosowaniu zintegrowanych nowoczesnych technologii detekcji pożaru.

5.5 Zakres ochrony

Przyjmuje się, że zakres ochrony to ochrona całkowita, w związku z czym zabezpieczeniu podlegają wszystkie ciągi komunikacyjne oraz wszystkie pomieszczenia w wyjątkiem pomieszczeń sanitariatów. Ochroną objęta została również kondygnacje strychu, która również została zabezpieczona czujkami optycznymi dymu. W obrębie klatek schodowych zostały rozmieszczone przyciski ręcznego ostrzegania pożarowego ROP. Zgodnie z zaleceniami konserwatora budynek Ratusza podlega ochronie konserwatorskiej, a trasy okablowania należy wykonać zgodnie z zaleceniami Opolskiego Wojewódzkiego Konserwatora Zabytków, a także w sposób, który ma zapewniać łatwe, bezkolizyjne i bezpieczne prowadzenie kabli uwzględniając inne instalacje w budynku. Okablowanie należy prowadzić w następujący sposób:

- Przewody instalacyjne prowadzić podtynkowo;
- Bruzdy ściennie należy uzupełnić tynkiem wapienno-piaskowym, bez domieszek cementu oraz pomalować w kolorystyce analogicznej do istniejącej;
- Wskazane jest prowadzenie tras kablowych w części przypodłogowej ścian;
- Nie dopuszcza się prowadzenia linii kablowych w obrębie zachowanych w budynku sklepień kolebkowych;
- W Sali obrad ochronie podlega bogata dekoracja sztukatorska na ścianach i sklepieniu oraz drewniane boazerie, w związku z powyższym linię kablową należy ulokować tak, aby zapewnić maksymalną ochronę substancji zabytkowej wyżej wymienionych elementów zdobniczych;

5.6 Opis systemu sygnalizacji pożaru

W instalacji dla budynku zaprojektowano system oparty na mikroprocesowej centrali detekcji pożaru z kolorowym wyświetlaczem i ekranem dotykowym 8,4 TFT. Główną cechą systemu jest

decyzyjność w podejmowaniu działań po stronie centrali, a nie elementów detekcyjnych. Wszelkie sygnały wpływające z elementów detekcyjnych znajdujących się na pętli są analizowane i przetwarzane przez procesor w celu podjęcia odpowiednich działań związanych z zaistniałą sytuacją. Centrala pracuje w układzie linii dozoru, pętlowych z możliwością indywidualnego adresowania wszystkich elementów. System ma mieć możliwość podłączenia modułów informacyjnych oraz sterująco-informacyjnych na magistrali zewnętrznej. System ma mieć możliwość podłączenia łącznie do 16 modułów rozszerzeń. Centrala sygnalizacji pożarowej z kolorowym wyświetlaczem i ekranem dotykowym ma być kompatybilna wstecz i umożliwić pracę ze starszymi systemami opartymi o moduł wyświetlacza operatora (z podświetlanym wyświetlaczem) oraz panelem operatora (ze wszystkimi przyciskami sygnalizacji pożarowej niezbędnymi dla operatora i diodami LED).

W przypadku zastosowania panelu wyniesionego, panel ma mieć - tak jak centrala kolorowy ekran dotykowy 8,4 TFT i ma posiadać wszystkie funkcje centrali. System ma posiadać urządzenie serwisowe, aby zaprogramować czujki, elementy liniowe i ręczne ostrzegacze pożarowe oraz sprawdzić poprawność ich działania. Ma być zapewniona możliwość komunikacji z czujką minimum na dwa sposoby: poprzez włożenie czujki do urządzenia serwisowego lub bezprzewodowo za pomocą podczerwieni. Komunikacja z ręcznymi ostrzegaczami pożarowymi i elementami liniowymi ma być realizowana za pomocą połączenia kablowego lub za pomocą podczerwieni (dla elementów liniowych z odpowiednim detektorem). Urządzenie serwisowe ma być zabezpieczone kodem dostępu oraz posiadać kolorowy ekran dotykowy.

System sygnalizacji pożaru ma mieć możliwość komunikacji z innymi systemami takim jak BMS, poprzez protokół BACnet lub innymi poprzez moduł MODBUS. Ma umożliwiać również podłączenie oprogramowania wizualizacyjnego, programów diagnostycznych umożliwiających serwisowanie i podgląd systemu, programów zdalnego dostępu oraz programów symulacyjnych sprawdzających zaprogramowane sterowania i działanie systemu. System ma posiadać również oprogramowanie weryfikujące prawidłowość doboru elementów systemu.

System sygnalizacji pożaru ma umożliwiać jednocześnie integrację z innymi systemami, tj. telewizją przemysłową, kontrolą dostępu, systemem przywoławczym za pomocą oprogramowania integrującego, które łączy funkcjonalność działania wszystkich tych elementów. Centrala ma mieć możliwość programowania za pomocą złącza RS232 lub portu USB. Połączenie central w sieci ma być możliwe za pomocą okablowania miedzianego lub światłowodowego. System ma obejmować swoim zakresem cały budynek i być zasilany prądem zmiennym 230V z wydzielonego pola rozdzielni głównej obiektu, sprzed wyłącznika głównego prądu. System sygnalizacji pożaru ma mieć możliwość wykorzystania pracy na okablowaniu ekranowanym, jak i nieekranowanym.

Centrala musi posiadać certyfikat wydany przez CNBOP z maksymalną ilością elementów na pętli dozoru do 250 elementów.

W skład systemu będą wchodziły następujące elementy:

- Centrala sygnalizacji pożaru
- Czujki wielodetektorowe dymu, temperatury i tlenku węgla
- Czujki optyczne dymu

- Ręczne ostrzegacze pożarowe
- Moduły wejść, wyjść (monitorujące, sterujące)
- Sygnalizatory optyczno-akustyczne pętlowe
- Sygnalizatory optyczno-akustyczne pętlowe w gnieździe czujki
- Bezprzewodowe urządzenie programująco-serwisowe

Linie dozоровe w konfiguracji pętli wraz z izolatorami zwarć zapewniają wysoką odporność systemu na uszkodzenia linii dozоровej. Czujki z izolatorami zwarć zostaną umieszczone w podstawach czujek z funkcją zachowania ciągłości pętli. Izolatory mają być umieszczone w czujkach, ROP i elementach sterujących i monitorujących i zostaną rozmieszczone zgodnie z zaleceniami producenta i obowiązującymi przepisami.

Centrala ma być wyposażona w panel z wyświetlaczem (kolorowym ekranem dotykowym) z możliwością logowania za pomocą kart zbliżeniowych RFID, i będzie umożliwiała wysłanie sygnału o pożarze i awarii do stacji monitorowania alarmów pożarowych.

Do wykrywania pożaru przewidziano zastosowanie czujek wielodetektorowych dymu, temperatury i tlenku węgla oraz optycznych czujek dymu. Zastosowane czujki przetwarzają informacje o stanie przestrzeni pomiarowej w formie analogowej, dzięki czemu czułość dostosowuje się do zmian środowiskowych.

Do wywołania alarmu pożarowego przez osoby przebywające w obiekcie przewidziano ręczne ostrzegacze pożarowe.

Centrala sygnalizacji pożarowej służąca do obsługi systemu, powinna zostać zamontowana w pomieszczeniu 1.19 na kondygnacji 0, w której stale przebywają ludzie i w sposób ciągły centrala nadzorowana jest przez odpowiednio przeszkoloną obsługę.

W pomieszczeniu, w którym zainstalowano centralę sygnalizacji pożarowej należy umieścić:

- plan sytuacyjny nadzorowanego obiektu;
- opis funkcjonowania i obsługi urządzeń sygnalizacji pożarowej;
- wskazówki, jak należy postępować w przypadku pożaru;
- książkę eksploatacji i konserwacji instalacji SSP, w której należy wpisywać:
 1. przeprowadzone kontrole instalacji;
 2. przeprowadzane naprawy;
 3. zmiany i uzupełnienia instalacji;
 4. wszystkie alarmy z podaniem daty, godziny i przyczyny ich wywołania.

Książkę taką należy prowadzić również w przypadku, gdy centrala sygnalizacji pożarowej jest wyposażona w pamięć zdarzeń i drukarkę.

5.7 Opis działania systemu

Elementy liniowe, zainstalowane w adresowalnej linii dozorowej, po odebraniu właściwego sygnału z centrali (adresu elementu), przesyłają zwrotne sygnały z informacją o swoim rodzaju i stanie. Wymiana informacji między elementami liniowymi i centralą odbywa się poprzez moduły główne. Po analizie odebranych sygnałów, moduł główny przekazuje odpowiednią informację poprzez magistralę centralową do głównego sterownika centrali CPU. Mikroprocesor sterownika informacje te przetwarza i wypracowuje odpowiednie sygnały dla pozostałych układów.

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

Dla transmisji informacji od i do centrali wykorzystywany jest szybki i niezawodny protokół pętlowy MX DIGITAL przekazujący do centrali wszystkie parametry w postaci analogowej. Pozwala to na pracę czujki w różnych trybach wykrywania pożaru, dobieranych w trakcie programowania pod kątem optymalizacji czułości i minimalizacji ryzyka alarmów fałszywych. W czujkach wielosensorowych wszystkie sensory mogą pracować jednocześnie, zaś oprogramowanie uwzględnia zależności pomiędzy ich parametrami.

Zasilacz sieciowy ma za zadanie dostarczenie roboczego napięcia centrali, a w razie braku zasilania sieciowego rolę tę pełni rezerwowa bateria akumulatorów.

5.8 Opis urządzeń

Adresowalny system sygnalizacji pożarowej to komplet urządzeń służących do wykrywania pożaru, powiadomienia odpowiednich służb interwencyjnych, włączenia urządzeń wykonawczych i rejestrowania występujących w systemie zdarzeń.

5.8.1 Centrala detekcji pożaru

Centrala jest urządzeniem wieloprocessorowym, gwarantującym niezawodną pracę systemu i dającym wiele udogodnień podczas programowania i późniejszej obsługi.

Centrala jest urządzeniem z podwójnym układem sterowników procesorowych, gwarantującym niezawodną pracę systemu i dającym wiele udogodnień podczas programowania i późniejszej obsługi. Centrala sygnalizacji pożarowej ma być zbudowana w oparciu o w pełni programowalny interfejs użytkownika z ekranem dotykowym 8,4" TFT. Dotykowy, kolorowy interfejs użytkownika ma posiadać ekran instrukcji dla operatora, ergonomiczny wyświetlacz ikon, diody LED podsumowujące informację o zdarzeniach. Logika pracy centrali ma być organizowana przez procesor z wgranymi schematami i automatyczny mechanizm, decydujący o wzbudzeniu alarmu pożarowego, oparty o algorytm weryfikujący cykl co najmniej kilku czynników detekcyjnych, sposobu i warunków ich wykrycia oraz progresu ich stanu. Zastosowanie wieloetapowego i wielopunktowego algorytmu detekcyjnego ma zapewnić najwyższą skuteczność i

jednocześnie maksymalnie zminimalizować współczynnik fałszywych alarmów wywoływanych przez system detekcji.

Centrala ma mieć możliwość obsługi do 240 stref, w które w sposób programowy są łączone czujki pożarowe, ręczne ostrzegacze pożarowe, elementy wejść i wyjść, moduły sterujące sygnalizatorami i inne moduły. Do każdej strefy lub sektora można przyporządkować komunikat umożliwiający lokalizację pożaru. Interfejs użytkownika ma mieć możliwość wgrania map obiektu (planów, rysunków pomieszczeń, zdjęć operatorów), które mogą być pokazywane w reakcji na zaprogramowane wcześniej zdarzenia, np. po zadziałaniu elementu detekcyjnego można wyświetlić na ekranie pomieszczenie, w którym wykryto zagrożenie, dzięki czemu lokalizacja pożaru jest jeszcze szybsza i dokładniejsza, co sprawia, że system jest bardziej bezpieczny i skuteczny – maksymalnie szybka reakcja na pożar i jego skuteczna lokalizacja graficzna w centrali. Do każdej strefy ma być możliwość wgrania do 10 map. Ekran dotykowy ma reagować na dotyk operatora, a nawet strażaka w rękawicach strażackich. Ponadto, ekran ma być personalizowalny przez wykorzystanie wygaszacza ekranu ze zdefiniowaną (wgraną) grafiką, np. wg preferencji Operatora, Użytkownika czy Serwisanta (np. logo firmy, etc). Centrala ma mieć możliwość obsługi 250 adresów na każdej pętli i przechowywać do 10000 zdarzeń. Centrala ma mieć możliwość zapisu zdarzeń, takich jak pożary, awarie, alarmy wstępne, ostrzeżenia, sterowania, czy stany elementów systemu (czujek, ROP-ów, elementów liniowych i innych) na zewnętrznym dysku pendrive podłączonym do złącza USB zlokalizowanego na przedniej ścianie urządzenia. W celu unifikacji i łatwości dostępu do danych plik wyjściowy ze zdarzeniami ma być w formacie txt. Gniazdo USB ma pozwalać również na wgranie konfiguracji programowej urządzenia. Centrala ma mieć możliwość autoryzacji i dostępu do określonego poziomu serwisowego za pomocą klucza, z użyciem hasła, a także za pomocą karty RFID (standard Mifare), która zapewnia natychmiastowy dostęp do menu, zalogowanie się i najszybsze podjęcie reakcji na zaistniałą sytuację. Zaprojektowana centrala pożarowa ma być wyposażona maksymalnie w 4 pętle. Ma również mieć możliwość współpracy z różnymi producentami peryferiów w ramach integracji sprzętowej, m.in.: umożliwiać podłączenie drukarki do portu COM1 czy zapewnić wykorzystanie sygnalizatorów nieadresowalnych (rozgłaszających komunikaty głosowe za pomocą modułów sterujących sygnalizatorami). Centrala ma mieć możliwość współpracy z różnymi elementami detekcyjnymi, typu czujki wielodetektorowe, trójdetektorowe, czujki liniowe, czujki płomienia z kamerami, czujki do stref zagrożonych wybuchem, czujki zasysające. Centrala ma mieć możliwość automatycznego wyprowadzenia sygnału do urządzeń transmisji alarmu do PSP.

Na płycie głównej centrali znajdują się następujące złącza:

§ Złącza adresowalnych linii czujek: pętla wraz z adresowalnymi czujkami dołączana jest do złącz linii czujek. Za pośrednictwem linii czujek następuje wymiana danych pomiędzy centralą a czujkami i modułami liniowymi. Ponadto złącze adresowalnych linii sygnałowych wyposażone jest w przekaźniki, które odłączają linię czujek w przypadku wystąpienia zwarcia (tzw. izolatory zwarc).

§ Na płycie głównej PFI800 znajdują się 4 złącza linii czujek. W zależności od konfiguracji systemu do pojedynczej linii można dołączyć maksymalnie 250 adresów na potrzeby urządzeń pętlowych

§ Wyjścia przekaźnikowe bezpotencjałowe: na płycie głównej znajdują się 4 przekaźniki. Dwa z nich stanowią ogólne przekaźniki alarmu (RL1) i uszkodzenia (RL2), możliwe do wykorzystania do przesyłania informacji o alarmach i usterkach do urządzenia transmisji alarmów pożarowych (UTA). Dwa pozostałe przekaźniki (RL3 i RL4) są do dowolnego wykorzystania.

§ Wyjścia dozorowane: dwa wyjścia dozorowane do wysterowania sygnalizatorów alarmowych (np. sygnalizatorów akustycznych, optycznych, itp.).

§ Wyjścia zasilające 24VDC: dwa wyjścia służące do zasilania urządzeń zewnętrznych (np. panele wyniesione, drukarki itp.)

§ Wejścia nadzorowane: dwa wejścia do dowolnego wykorzystania

§ Wejścia izolowane: dwa wejścia typu optoizolator, służące do nadzorowania napięcia zewnętrznego 24VDC

§ Wejście typu emergency: służące do aktywacji trybu pracy awaryjnej centrali

§ Porty szeregowo: płyta główna centrali posiada 3 łącza szeregowo RS-232, służące do komunikacji z następującymi urządzeniami:

- o Poprzez wyjście COM1 – drukarka szeregowo
- o Poprzez wyjście COM2 – komputer konfigurujący / modem
- o Poprzez wyjście COM3 – drukarka szeregowo

§ Port USB – do przesyłania konfiguracji / firmware'u do centrali

§ Port Ethernet – do dołączenia graficznego interfejsu użytkownika GUI oraz paneli wyniesionych

§ Magistrala zewnętrzna (Remote-Bus): magistrala zewnętrzna to zbiorcza linia magistrali asynchronicznej RS-485 (maksymalna długość wynosi 1200 m). Do zewnętrznej magistrali można dołączyć maksymalnie 15 kolejnych modułów. Adresy modułów ustawiane są za pomocą mikroprzełączników. Maksymalna liczba wejść i wyjść możliwych do dołączenia do modułów magistrali zewnętrznej jest ograniczona przez punkty danych obsługiwane przez moduł MPM800.

§ Wewnętrzna magistrala sterowania (magistrala we-wy Local I/O): do wewnętrznej magistrali sterowania centrali można dołączyć maksymalnie 2 moduły wejścia-wyjścia IOB800. W drugim z modułów IOB800 można jednak wykorzystać tylko 8 wyjść. Magistrala jest dwukierunkową szyną 1-bitową z możliwością adresowania 24 urządzeń wejścia-wyjścia. Przykładowo można ją wykorzystać do wysterowania 16 zewnętrznych diod LED, przekaźników, itd. i do odczytu max. 8 wejść dodatkowych. Maksymalna długość kabli wewnętrznej magistrali sterowania wynosi 2 m (do każdego z modułów lub jako długość całkowita przy modułach łączonych kaskadowo).



Rys.4 – widok centrali

Centrala obsługuje do 240 stref, w które w sposób programowy łączone są czujki pożarowe. Rozwiązanie to zapewnia proste i tanie zmiany w oprogramowaniu centrali (bez konieczności ingerencji w strukturę linii dozorowych) w razie ewentualnych zmian dotyczących adaptacji pomieszczeń. Dla każdej strefy dozorowej lub sektora (jednostka łącząca w sobie jedną lub więcej stref) można przyporządkować komunikat ułatwiający lokalizację pożaru.

Konfiguracja centrali

- Wyposażenie standardowe centrali:
 - obudowa kompletna z kasetą na 4 wtykowe karty rozszerzeń
 - płyta główna centrali z wbudowanym procesorem głównym, kością pamięci oraz ładowarką baterii
 - zasilacz sieciowy 24V 5A zlokalizowany w obudowie centrali
 - panel dotykowy z polem obsługi i wskazań - GUI
- Wyposażenie dodatkowe (opcjonalne):
 - karta sieciowa
 - karta pętli dozorowych
 - karta ładowarki i nadzoru dodatkowego zasilacza i baterii
 - dodatkowa obudowa rozszerzeń z zasilaczem 5A
 - dodatkowa obudowa rozszerzeń(pusta)
 - panel wskazań diodowy na 40 stref
 - panel wskazań diodowy na 80 stref
 - drukarka
 - moduł bezpieczników
 - moduł 8 wejść / 8 wyjść
 - switch służący do dołączenia paneli wyniesionych

Parametry centrali

- | | |
|--|----------------------------|
| · zasilanie podstawowe sieciowe: | 230V, 50Hz |
| · zasilanie rezerwowe wewnętrzne: | bateria akumulatorów 24VDC |
| · przełączanie na zasilanie rezerwowe: | automatyczne |

- przełączanie na ładowanie akumulatorów: automatyczne
- maksymalna rezystancja linii dozorowej: 146 Ω
- maksymalna pojemność linii dozorowej: 225nF/km
- ilość linii dozorowych adresowalnych: do 8
- maksymalna ilość adresów w jednej pętli: do 250
- liczba stref: do 240
- magistrala REMOTE BUS: długość do 1200m,
- wyświetlacz: dotykowy, rezystancyjny
- wyjścia dozorowane: 2 po 3A
- wejście dozorowane: 2
- wejście niedozorowane: 2
- wyjście alarmu: 1 zestyk 1A/30V
- wyjście uszkodzenia: 1 zestyk 1A/30V
- poziomy (uprawnienia) dostępu: 8
- możliwość pracy w sieci
- możliwość podłączenia drukarki
- możliwość podłączenia paneli wyniesionych
- miejsce na dodatkowe moduły
- miejsce na 2 akumulatory 12V/38Ah wewnątrz obudowy centrali

5.8.2 Czujka wielodetektorowa dymu, temperatury i tlenku węgla

Czujka jest adresowalną wielodetektorową czujką dymu, temperatury i tlenku węgla. Elementem pomiarowym w czujce jest układ optyczny działający na zasadzie światła rozproszonego, układ temperaturowy i tlenku węgla. Czujka posiada możliwość programowania poziomów zadziałania, w zależności od warunków pracy lub eksploatacji. Ma też możliwość raportowania stanu zabrudzenia do centrali pożarowej. Może pracować w zakresie temperatur od -25 °C to +70 °C i wilgotności do 95%. Czujka ma być programowana a sprawdzanie poprawności działania ma się odbywać za pomocą urządzenia serwisującego poprzez wkręcenie do urządzenia lub bezprzewodowo za pomocą podczerwieni. Czujka ma posiadać diodowe wskaźniki LED (czerwone, pomarańczowe) informujące o stanach jej pracy, jak normalna praca (miganie na czerwono), zadziałanie (dioda LED świeci na czerwono) czy usterka, odłączenie (Dioda LED świeci na pomarańczowo). Wszystkie czujki mają być wyposażone w izolatory zwarć, zapewniając wysoką odporność systemu na uszkodzenia linii dozorowej. Gniazda do czujek z izolatorami zwać mają posiadać przełącznik, który utrzymuje złącze otwarte, pozwalając na prawidłową pracę wbudowanego izolatora zwarcia w czujce, natomiast po usunięciu czujki z gniazda przełącznik ma zamykać złącze, gwarantując ciągłość okablowania pętli bez czujki. Aby dostosować się do zmian otoczenia w budynkach, czujka ma mieć możliwość wyboru innej pracy elementów detekcyjnych w zależności od trybu nocnego lub dziennego – poprzez automatyczną zmianę czułości detektorów. Czujka ma mieć możliwość pracy w następujących ustawieniach:

- Tryb 0 – Tryb uniwersalny – Maksymalna ochrona poprzez trzy elementy detekcyjne wprowadzające sygnał do algorytmu detekcji. Czułość każdego elementu regulowana

automatycznie w odpowiedzi na sygnały z czujników w celu zapewnienia szybkiego i niezawodnego wykrycia szerokiej gamy rodzajów pożaru.

- Tryb 1 – Tryb odporny – Maksymalna odporność na fałszywe alarmy, wykorzystująca wszystkie trzy elementy w sposób podobny do trybu uniwersalnego. Nacisk położony jest na zerowy poziom fałszywych alarmów i jest przeznaczony do wykorzystania w trudniejszych warunkach lub tam, gdzie obciążenie może być problematyczne.
- Tryb 2 - A1R (A1R - czujka różnicowa temperatury).
- Tryb 3 - HPO + A1R normalna czułość (HPO – tryb optyczny o czułości zależnej od wzrostu temperatury).
- Tryb 4 - CCO normalna czułość (CCO – tryb tlenku węgla CO o czułości zależnej od wzrostu temperatury).
- Tryb 5 – Detektor toksycznego gazu tlenku węgla

5.8.3 Czujka optyczna dymu

Czujka jest adresowalną optyczną czujką dymu. Elementem pomiarowym w czujce jest układ optyczny działający na zasadzie światła rozproszonego. Czujka posiada możliwość programowania poziomów zadziałania, w zależności od warunków. Ma też możliwość raportowania stanu zabrudzenia do centrali pożarowej. Może pracować w zakresie temperatur od -25 °C to +70 °C i wilgotności do 95%. Czujka może być programowana i sprawdzana poprawność działania za pomocą urządzenia serwisującego poprzez wkręcenie do urządzenia lub za pomocą podczerwieni. Czujka ma posiadać diodowe wskaźniki LED (czerwone, pomarańczowe) informujące o stanach jej pracy, jak normalna praca (miganie na czerwono), zadziałanie (dioda LED świeci na czerwono) czy usterka, odłączenie (Dioda LED świeci na pomarańczowo). Czujki mają być wyposażone w izolatory zwarcia zapewniające wysoką odporność systemu na uszkodzenia linii dozoru. Gniazda do czujek z izolatorami zwać mają posiadać przełącznik, który utrzymuje złącze otwarte, pozwalając na prawidłową pracę wbudowanego izolatora zwarcia w czujce, natomiast po usunięciu czujki z gniazda przełącznik zamyka złącze, zapewniając ciągłość okablowania pętli bez czujki. Aby dostosować się do zmian w budynkach, czujka ma mieć możliwość wyboru pracy innej czułości w zależności od trybu nocnego lub dziennego – automatyczna zmiana pracy czułości czujki. Czujka ma mieć możliwość pracy w trzech ustawieniach czułości elementu detekcyjnego:

- Niska czułość.
- Średnia czułość.
- Wysoka czułość

5.8.4 *Moduł monitorująco-sterujący*

Moduł monitorująco-sterujący jest adresowalnym urządzeniem pętlowym wyposażonym w cztery wejścia przeznaczone do nadzorowania zestyków zwrotnych bądź rozdzielników, z możliwością kontroli stanu linii i sygnalizacji jej uszkodzeń (zwarcie lub przerwa) oraz cztery swobodnie programowalne przekaźniki zawierające przełączalne zestyki bezpotencjałowe. Zestyki przekaźników są odseparowane galwanicznie od reszty systemu. Stan przekaźników jest nadzorowany – wykrywane i sygnalizowane są stany aktywny, nieaktywny oraz sklejenie się zestyku. Moduł wyposażony jest w diodę świecącą LED, wskazującą jego stan. Moduł posiada wbudowany izolator zwarcia. W zależności od aplikacji, moduł pozwala też dołączyć zewnętrzne zasilanie o napięciu 24 lub 48 VDC, którego obecność jest nadzorowana przez moduł.

W zależności od konfiguracji, moduł ten może zajmować na pętli dozorowej od 2 do 8 adresów.

5.8.5 *Gniazda czujek*

Czujki serii 850 mogą być instalowane w gniazdach 4-calowych. Gniazdo jest podstawowym gniazdem montażowym przeznaczonym do montażu czujek 6 generacji, serii posiadających wbudowane izolatory zwarcia. Gniazdo dzięki swojej konstrukcji zapewnia utrzymanie ciągłości pętli dozorowej nawet w przypadku demontażu czujki. Pozwala to na sprawne uruchomienie i dokonanie pomiarów elektrycznych pętli dozorowej jeszcze przed zamontowaniem urządzeń.

5.8.6 *Ręczny ostrzegacz pożaru*

ROP jest przeznaczony do przekazywania informacji o pożarze do współpracującej centrali sygnalizacji pożarowej przez osobę, która zauważyła pożar i ręcznie uruchomiła ostrzegacz (zbiła szybkę). Ostrzegacze mogą pracować wyłącznie na pętlach dozorowych central systemu detekcji pożaru. Ostrzegacz przeznaczony jest do montażu wewnątrz obiektów i jest wyposażony w wbudowany izolator zwarcia. Dodatkowo posiada mechanizm pozwalający na testowanie urządzenia przy pomocy specjalnego klucza testowego, bez konieczności zbijania szybki.

5.8.7 *Sygnalizator*

Adresowalny pętlowy sygnalizator optyczno-akustyczny z zespołem diod LED. Posiada możliwość wyboru jednego z 16 różnych sygnałów akustycznych, 2 programowalne poziomy głośności, 2 programowalne częstotliwości migania. Wybieranie tonu, głośności i częstotliwości migania za pomocą oprogramowania do konfiguracji centrali. Sygnalizatory należy zainstalować na pętli dozorowej i zaadresować zgodnie z konfiguracją centrali. Sygnalizatory zainstalowane będą na pętli wykonanej kablem ognioodpornym typu HTKSH PH90 o odpowiednim przekroju żyły w zależności od obciążenia i długości linii. Zasilanie i transmisja danych z pętli. Wbudowany izolator zwarcia

Sygnalizatory muszą być wyposażone w mechanizm monitorowania dźwięku odbitego (RSM) i być monitorowane elektronicznie przez centralę, a także wyposażone w automatyczny test własny. Sygnalizatory muszą być wyposażone w wbudowany izolator zwarć.

5.8.8 Sygnalizator w gnieździe

Adresowalny pętlowy sygnalizator optyczno-akustyczny z zespołem czerwonych diod LED umieszczony w gnieździe czujki. Posiada możliwość wyboru jednego z 15 różnych sygnałów akustycznych, 4 programowalne poziomy głośności, 2 programowalne częstotliwości migania. Wybieranie tonu, głośności i częstotliwości migania za pomocą oprogramowania do konfiguracji centrali. Sygnalizatory należy zainstalować na pętli dozorowej i zaadresować zgodnie z konfiguracją centrali. Sygnalizatory mogą być zainstalowane będą na pętli wykonanej kablem ognioodpornym typu HTKSH PH90 o odpowiednim przekroju żyły w zależności od obciążenia i długości linii. Zasilanie i transmisja danych z pętli. Wbudowany izolator zwarć

Sygnalizatory muszą być wyposażone w mechanizm monitorowania dźwięku odbitego (RSM) i być monitorowane elektronicznie przez centralę, a także wyposażone w automatyczny test własny. Sygnalizatory muszą być wyposażone w wbudowany izolator zwarć.

5.8.9 Urządzenie programująco-serwisujące

Za pomocą urządzenia serwisującego można programować czujki, elementy liniowe oraz ROPy, jak również sprawdzić poprawność ich działania. Urządzenie przechowuje informację z uruchomienia i testowania na pamięci USB oraz pozwala na generowanie raportów w formie elektronicznej. Urządzenie komunikuje się z czujką na dwa sposoby: poprzez włożenie czujki do urządzenia lub za pomocą podczerwieni. Urządzenie zabezpieczone jest pinem dostępu. Posiada ekran dotykowy.

5.9 Podział na strefy dozorowe

Aby ułatwić przyporządkowanie poszczególnych elementów pętlowych systemu do odpowiednich obszarów budynku wprowadzono podział poszczególnych stref pożarowych na strefy dozorowe. Opisy w centrali dla czujek, ROPów oraz modułów pętlowych powinny odpowiadać wprowadzonemu podziałowi. W przypadku zmian nazw lub numeracji stref dozorowych na etapie wykonawczym lub w czasie eksploatacji budynku, należy je również wprowadzić do dokumentacji powykonawczej oraz odpowiednio uaktualnić w centrali SSP.

STREFA POŻAROWA NR:

01 – Kondygnacja -1 oraz 0

02 – Kondygnacja +1

03 – Kondygnacja +2 oraz Strych

5.10 Sterowanie i monitorowanie urządzeń zabezpieczenia pożarowego budynku

Zakłada się, że w przypadku wystąpienia pożaru w budynku, system sygnalizacji pożaru będzie spełniał następujące

funkcje sterownicze:

- zwolnienie elektrozamykaczy drzwi pomieszczeń 1.7 oraz 1.19
- wystawianie sygnalizatorów optyczno-akustycznych
- umożliwienie automatycznego wyprowadzenia sygnału do urządzeń transmisji alarmów do centrum monitoringu
- wystawianie detektora gazu w piwnicy budynku w celu odcięcia dopływu gazu do budynku

W przypadku pojawienia się alarmu II stopnia przewiduje się uruchomienie sygnalizacji akustycznej w budynku. Wystawianie sygnalizatorów odbywać się będzie za pomocą wystawiania adresowalnych sygnalizatorów zainstalowanych na pętlach dozorowanych z centrali pożarowej.

Funkcje sterownicze zostaną zrealizowane za pomocą modułów sterujących instalowanych na liniach dozorowych.

5.11 Sterowanie sygnalizacją akustyczno-optyczną

W przypadku pojawienia się alarmu II stopnia przewiduje się uruchomienie sygnalizacji akustyczno-optycznej w budynku. Wystawianie sygnalizatorów odbywać się będzie na dwa sposoby. Na zewnątrz budynku sygnalizator zostanie uruchomiony za pomocą wyjścia dozorowanego w centrali pożarowej. Na kondygnacjach budynku zaprojektowano sygnalizatory pętlowe, które mogą być uruchomione w każdej ze stref niezależnie. Sygnalizatory pętlowe akustyczno-optyczne posiadają wbudowany czujnik optyczny oraz mikrofon, które umożliwiają wykonanie co rocznych prób zadziałania sygnalizatorów w przeciągu 1 min na całym budynku.

Zgodnie z polskimi normami i przepisami poszczególne urządzenia muszą posiadać certyfikaty, świadectwa kwalifikacyjne, homologację oraz świadectwa o dopuszczeniu do stosowania w Polsce, wydane przez stosowne instytucje. W przypadku systemów sygnalizacji pożaru taką instytucją jest Centrum Naukowo Badawcze Ochrony Przeciwpożarowej w Józefowie.

5.12 Organizacja alarmowania

Centrala rozróżnia trzy rodzaje alarmów:

- alarm z czujki automatycznej,
- alarm z ręcznego ostrzegacza pożarowego,
- alarm z czujnika detekcji gazu,

Centrala sygnalizuje alarmy:

- pożarowy I stopnia,
- pożarowy II stopnia,
- uszkodzeniowy.

Alarm z ostrzegaczy ręcznych jest sygnalizowany w centrali od razu jako alarm II stopnia.

5.13 Tryby pracy

W zależności od zaprogramowania system może być przystosowany do jednego lub dwóch trybów pracy, czyli do trybu nocnego lub trybu dziennego i nocnego. Jeśli system przystosowano do trybu pracy dziennej i nocnej, przełączanie trybów może odbywać się automatycznie przez sterowanie czasowe lub za pomocą przycisku.

Tryb nocny

Każdy z alarmów pochodzący z czujek jest od razu traktowany jako ALARM II STOPNIA. W wyniku alarmu całkowicie automatycznie następuje wystawienie wszystkich urządzeń przeciwpożarowych, zgodnie z zaprogramowanym algorytmem działania, oraz uruchomienie przekaźnika alarmu pożarowego (przekazanie alarmu do PSP).

Tryb dzienny

W trybie pracy dziennej niezbędna jest obecność przeszkolonego oraz dostępnego w trakcie czasu opóźnienia personelu obsługi.

Po zadziałaniu elementu liniowego w adresowalnej linii dozorowej centrala, na podstawie algorytmów decyzyjnych, sygnalizuje ALARM I STOPNIA lub ALARM II STOPNIA w zależności od wariantów alarmowania zaprogramowanych dla konkretnych stref. Po wystąpieniu alarmu I stopnia (pobudzenie czujki) system pracujący w trybie dziennym przechodzi w tzw. układ interwencji. Alarm I stopnia sygnalizowany jest w centrali świeceniem czerwonych wskaźników „POŻAR” w module obsługi.

Na wyświetlaczu LCD w polu „POŻAR” pojawia się komunikat zawierający:

- numer strefy i elementu (czujki) w stanie alarmu;
- opis strefy dozorowej (zdefiniowany podczas konfiguracji);
- opis elementu (zdefiniowany podczas konfiguracji);
- typ alarmu;
- tekst komentarza lub data, godzina i typ czujki;
- temperatura rzeczywista, jeśli dana czujka wyposażona jest w czujnik temperatury.

Alarm I stopnia jest alarmem wewnętrznym i wymaga zawsze zgłoszenia się personelu dyżurującego i potwierdzenia alarmu przyciskiem „ROZPOZNANIE” (w czasie T1) oraz rozpoznania zagrożenia w obiekcie (czas T2). W czasie T2 jest możliwość skasowania alarmu przyciskiem „KASOWANIE”, jeśli obsługa uzna, że nie ma zagrożenia. Do tego momentu centrala sygnalizuje alarm I stopnia. Podczas, gdy obsługa ma czas na rozpoznanie naciśnięcie któregośkolwiek ROP-a wywołuje od razu alarm II stopnia. Jeśli brak jest odpowiedniej reakcji dyżurującego personelu na alarm I stopnia, wówczas wywoływany jest alarm II stopnia.

Alarm II stopnia jest wewnętrznym stanem centrali, który powoduje, oprócz wywołania w centrali sygnalizacji optycznej i akustycznej, przekazanie na zewnątrz sygnału o pożarze (zadziałanie wyjść zadeklarowanych jako wyjścia do urządzeń transmisji alarmu) oraz uruchomienie dodatkowych wyjść, których występowanie uwarunkowane jest wystąpieniem alarmu II stopnia.

Wystąpienie w centrali alarmu II stopnia powoduje automatyczne przejście stref będących w alarmie I stopnia w stan alarmu II stopnia. Alarm II stopnia może być poprzedzony alarmem I stopnia lub jest generowany natychmiastowo w zależności od zaprogramowanego wariantu alarmowania dla konkretnej strefy w obiekcie lub trybu pracy centrali. Alarm II stopnia jest wezwaniem do natychmiastowego podjęcia akcji gaśniczej.

Jednocześnie z sygnalizacją optyczną, podczas alarmu pożarowego uruchamia się w centrali ciągły sygnał akustyczny, który można wyłączyć wciskając przycisk „WYCISZENIE.” Przechodzenie następnych stref w stan alarmu, zarówno w przypadku alarmu I stopnia, jak i alarmu II stopnia, ponawia sygnalizację akustyczną.

Resetowanie centrali odbywa się po naciśnięciu przycisku „KASOWANIE ALARMU”. Wyświetlacz LCD powraca do normalnego wskazania, o ile nie występują uszkodzenia lub inne zdarzenia. Resetowanie centrali można wykonać wyłącznie po ustaleniu źródła pożaru przez straż pożarną lub inne służby i opanowaniu sytuacji.

Uruchomienie ręcznego ostrzegacza pożaru wywołuje od razu ALARM II STOPNIA.

5.14 Montaż instalacji i prowadzenie okablowania

1. Montaż wykonywać zgodnie z obowiązującymi w kraju normami i przepisami. Uwagi odnośnie montażu okablowania i urządzeń. Celem uniknięcia kolizji zaleca się przeprowadzenie montażu instalacji SSP skoordynowany z innymi branżami. Sposób wykonywania połączeń między elementami linii podano na rysunkach instalacji.
2. Połączenia pętli dozorowych (linii wykonawczych, sterujących, sygnalizacyjnych) wykonać kablem dwużyłowym typu HTKSH PH90. Przewody układać podtynkowo, zgodnie z certyfikatem kabla.

Sposób układania przyjąć taki sam jak dla instalacji elektrycznych zachowując zgodność z certyfikatem kabla.

3. Obwody linii wykonawczych (sterujących) wykonać kablem – ilość żył i przekrój pojedynczej żyły uzależniony od podłączanych urządzeń i odległości. Przewody układać podtynkowo, zgodnie z certyfikatem kabla.

4. Line sygnalizatora zewnętrznego podłączyć do linii sygnalizatorów LS1 centrali pożarowej kablem niepalnym HTKSH PH90.

5. Czujki instalować zawsze bezpośrednio na stropie. Czujki zaleca się łączyć w podanej (rosnącej) kolejności numeracji. Podczas montażu sprawdzać numerację i nazwy pomieszczeń. Dane te są niezbędne do wykonania opisu tekstowego w centrali. Nazwy pomieszczeń, ich numerację oraz nazwy stref określać w porozumieniu z Zamawiającym (Użytkownikiem).

6. Moduły sterujące umieścić w sposób umożliwiający dostęp podczas serwisów i przeglądów zgodnie z rozmieszczeniem na rzutach budynku odpowiadającym wysterowaniu elementów na danej kondygnacji.

- Przewody prowadzić:
 - na kondygnacji -1 zgodnie z istniejącymi instalacjami w rurach osłonowych;
 - na kondygnacjach 0, 1, 2 oraz w pionach na wszystkich kondygnacjach podtynkowo,
 - na kondygnacji strychu w rurach osłonowych;
- Numerację linii i czujek podaną w projekcie należy traktować jako tymczasową.
- Moduły pętlowe instalować w miejscach umożliwiających przegląd i konserwację
- W przypadkach kolizji lub zbliżeń zachować odległość 50 cm czujek od ścian, podciągów, przewodów wentylacyjnych (o ile przebiegają one w odległości mniejszej niż 15 cm od stropu), opraw świetlnych itp. Zachować odległość czujek min. 1,5 m od kratki wentylacyjnych nawiewu i wywiewu.
- Zachować odległość min. 30 cm przewodów instalacji SSP od innych przewodów i kabli elektrycznych.
- Początki i końce linii dozorowych prowadzone w częściach pionowych instalacji prowadzić w osobnych rurach, przy czym dopuszcza się stosowanie wspólnej rury dla „początków” i wspólnej rury dla „końców” linii pętlowych.
- Montaż poszczególnych urządzeń podano w kartach technicznych wybranego urządzenia.

Wszystkie zmiany powstałe podczas montażu instalacji należy nanieść w dokumentacji powykonawczej.

5.15 Zasilanie podstawowe

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

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

Połączenie kablowe wykonać jako nierozłączne, kablem energetycznym ognioodpornym z oddzielnym zabezpieczeniem w rozdzielni głównej. Stosować odpowiednie zasady ochrony przeciwporażeniowej.

5.16 Zasilanie awaryjne

Projekt przewiduje zastosowanie central SSP wyposażonych w zasilanie akumulatorowe zapewniające pracę przez 72h dla stanu czuwania i 0,5h dla stanu alarmu.

Obliczenia zasilania awaryjnego

Minimalna pojemność akumulatorów C_{min} , przeznaczonych do zasilania urządzeń podanych w tabelach 1 i 2, przy następujących parametrach: $C_{mm} = k(I \cdot t_x + I_2 \cdot t_2)$

$\frac{3}{4}$ t – praca ciągła w stanie spoczynku 72h

$\frac{3}{4}$ t – praca ciągła w stanie alarmu 0,5h

$\frac{3}{4}$ k – współczynnik uwzględniający sprawność akumulatora $k=1,25$

I_1 – sumaryczny prąd spoczynkowy

I_2 – sumaryczny prąd w stanie alarmowania

Obliczenia zasilania awaryjnego central SSP dokonano w oprogramowaniu dostarczonym przez producenta systemu i przedstawiono poniżej.

Czas czuwania: 72h

Czas alarmu: 0,5h

Współczynnik wykorzystania baterii: 1,25

Min. pojemność baterii: 47,37 Ah

Obciążenie 40V: 0,63A

Obciążenie 24V: 0,42A

Suma obciążeń w stanie czuwania : 0,51A

Suma obciążeń w stanie alarmu : 1,40A

Suma obciążeń 24V : 1,44A

W celu zapewnienia podtrzymania zasilania rezerwowego w określonym w projekcie zakresie, centralę należy doposażyć w dodatkowy zasilacz w obudowę na akumulatory oraz zestawem akumulatorów. Dodatkowy zasilacz stanowi integralną część centrali pożarowej projektowanej w obiekcie i jest instalowany w dolnej części centrali.

5.17 Zalecenia dla wykonawcy i inwestora

ZALECENIA DLA WYKONAWCY

Przed przystąpieniem do robót należy

- Zapoznać się z projektem i ewentualne uwagi zgłosić projektantowi
- Zapoznać się z dokumentacją istniejących w obiekcie instalacji elektrycznych, wodnych, wentylacyjnych, oświetleniowych i innych w celu uniknięcia uszkodzeń i kolizji z tymi instalacjami oraz prawidłowego wykonania instalacji sygnalizacyjnej.
- Przewody typu PH90 mocować przy pomocy uchwytów E90 montowanych do ścian przy pomocy stalowych tulejek rozporowych oraz stalowych śrub klasy E90.
- Wykonawcę realizującego budowę niniejszego systemu, obowiązuje w jego zakresie przestrzeganie przepisów BHP i ppoż. W odniesieniu do wszystkich szczegółów, które w projekcie nie mogły być omówione.
- Instalację wykonać wg dostarczonych z urządzeniami DTR oraz zgodnie z odpowiednimi aprobatami technicznymi.
- Wszystkie odstępstwa należy uzgadniać z osobą pełniącą nadzór.
- Zapewnić zgodność instalacji z wymogami prawa, przepisów budowlanych, przepisów pożarowych
- Wszystkie przejścia instalacyjne przez granice stref pożarowych wypełnić masą ogniochronną o odporności właściwej dla przegrody i odpowiednio oznaczyć

- Po wykonaniu instalacji, należy poddać system testom prawidłowego działania, należy przeprowadzić:
 - a. Próbę działania wszystkich czujek pożarowych
 - b. Próbę działania wszystkich przycisków oddymiania i ręcznych ostrzegaczy pożarowych
 - c. Ocenę działania zasilacza i akumulatorów

Obowiązkiem wykonawcy jest wykonać instalację zgodnie w wszystkich obowiązującymi w momencie wykonania przepisami, normami, rozporządzeniami i wytycznymi.

ZALECENIA DLA INWESTORA

Obowiązkiem inwestora, Użytkownika oraz firmy wykonującej instalację jest zapewnienie poprawnego działania instalacji alarmowej poprzez:

- Przeszkolenie personelu obsługującego system
- Eksploatację zgodnie z przeznaczeniem systemu
- Systematyczną konserwację urządzeń
- Szybką naprawę i usuwanie usterek powstałych w trakcie eksploatacji systemu
- Należy dostosować instrukcję pożarową dla obiektu z uwzględnieniem konieczności otworzenia drzwi wskazanych w projekcie jako zapewniające dopływ świeżego powietrza uzupełniającego do oddymianej klatki schodowej.
- Wykonanie i konserwację zaprojektowanego systemu należy zlecić wyspecjalizowanej firmie. Wykonawca powinien być przeszkolony i akceptowany przez producenta lub dystrybutora systemu.

Podczas prowadzenia prac wykonawczych należy zapewnić:

§ - nadzór autorski

§ - nadzór inwestorski (wskazany jest inspektor posiadający wiedzę w zakresie ochrony p.poż)

Wykonawca systemu powinien złożyć Deklarację Zgodności Instalacji

Odbiór instalacji powinien odbywać się po wykonaniu całego systemu zgodnie z opracowaną dokumentacją techniczną i ewentualnymi zmianami wpisanymi do dziennika budowy. W odbiorze powinien uczestniczyć inspektor Państwowej Straży Pożarnej, wykonawca, oraz ewentualnie przedstawiciel firmy ubezpieczeniowej, Odbiór instalacji powinien być połączony z przekazaniem instalacji do eksploatacji. W odbiorze powinien uczestniczyć również konserwator systemu, który będzie sprawował nadzór nad eksploatacją systemu.

Należy zawrzeć umowę określającą zasady konserwacji, w tym czas usuwania usterek i czasookres konserwowania systemu.

6 Integracja systemów

W celu maksymalizacji funkcjonalności systemów oraz efektywności wykorzystania ich możliwości, systemy KD, CCTV, SSWiN i SSP występujące w projekcie zostały zaprojektowane w taki sposób, aby możliwa była współpraca między nimi oraz aby systemy wchodziły w interakcję między sobą. W projekcie uwzględniono zatem wszelkie konieczne interfejsy między systemami zarówno programowe jak i fizyczne zapewniające kompatybilność między systemami.

Security Management System (SMS) to w pełni konfigurowalna aplikacja która zawiera dynamiczne przetwarzanie alarmów, konfigurowalne alarmy i obsługę zdarzeń, raportowanie, eskalację alarmów, mechanizm przyczyn i skutków zdarzeń, wbudowany interfejs wideo (Video Micro-Viewer) i wiele innych w celu zapewnienia w pełni skalowalnego, wielooperatorskiego i wielomonitorowego systemu zarządzania bezpieczeństwem w budynku.

Wizualne i dźwiękowe powiadomienia o zdarzeniach, mapy graficzne oraz pełne funkcjonalne stanowisko dowodzenia; operator otrzymuje w pełni funkcjonalne narzędzie do kontroli w jednym zaawansowanym interfejsie użytkownika, dzięki czemu umożliwia personelowi ochrony zidentyfikowanie zdarzeń i reagowanie na nie w czasie rzeczywistym, na czas i zgodnie z priorytetem. Pomaga w ograniczeniu czasów reakcji na krytyczne zdarzenia i upraszcza operacje związane z bezpieczeństwem, jednocześnie zwiększając wizualizację zdarzeń i odpowiedzialność za alarm.

6.1 Integracja systemów

Główne wymagania dla systemu SMS

- **Aplikacja Command and Control**
 - system SMS musi umożliwiać monitorowanie i kontrolowanie korzystając z jednej, ujednoliconej platformy, która pomaga utrzymać niskie koszty operacyjne i zapewnia szybkie i skuteczne zarządzanie alarmami i zdarzeniami.
- **Scentralizowana aplikacja do centralnego zarządzania alarmami dla kontroli dostępu, CCTV, SSWiN oraz SSP**
- **Alarmy i urządzenia**
 - system SMS musi posiadać aplikację alarmową wyświetlającą informacje o typie alarmu, opisie alarmu, adres urządzenia, poziom priorytetu, czas alarmu, stan, powiązane wideo i adresata alarmu (dla systemów wielu użytkowników, gdzie więcej niż jeden operator może zarządzać alarmami). Operatorzy za pomocą jednego kliknięcia w alarm muszą mieć możliwość wyświetlić lokalizację danego urządzenia bezpośrednio na mapie graficznej, odczytać jego dane oraz wygenerować raport

urządzenia a także z odpowiednim poziomem autoryzacji izolować urządzenie. Izolacja urządzeń pozwala operatorom zablokować wszelkie dalsze alarmy występujące na danym urządzeniu, co jest idealne w momencie konserwacji urządzenia. Operatorzy muszą mieć możliwość wybrania dowolnego alarmu i zainicjować aplikację przetwarzania alarmu, która dostarczy im zestaw instrukcji, które muszą wykonać, aby potwierdzić alarm, a następnie zresetować alarm, jeśli to jest dozwolone. System musi zapewniać operatorom funkcję, która będzie wyświetlać informacje o wszystkich urządzeniach podłączonych do platformy SMS, takich jak Typ urządzenia, Opis urządzenia, Całkowita liczba alarmów, Pierwszy i Ostatni czas alarmu oraz informacje o tym, czy alarm został przefiltrowany lub izolowany dając operatorom pełny wgląd w stan wszystkich alarmów i urządzeń w czasie rzeczywistym.

- **Zaawansowane funkcje przetwarzania alarmów**

- aplikacja przetwarzania alarmów jest dedykowanym interfejsem dla operatorów systemu, którzy przeglądają szczegółowe informacje o alarmach systemowych i przetwarzają te alarmy w celu ich potwierdzenia i zresetowania. Operatorzy systemu muszą mieć możliwość wyświetlania wielu alarmów w różnych zakładkach w aplikacji do przetwarzania alarmów gdzie zostaną im przedstawione informacje na temat typu alarmu, daty / czasu wystąpienia zdarzenia, poziomu priorytetu i lokalizacji (dostępna jest karta mapy, aby wyświetlić SnapShot lokalizacji urządzenia na mapach graficznych, jeśli dotyczy). W informacjach o historii urządzeń muszą wyświetlać się wszystkie aktywne alarmy dla tego urządzenia, podając w czasie rzeczywistym stany alarmowe systemów bezpieczeństwa. Jeśli zdefiniowano Workflow, zostaną one również przedstawione wszystkim operatorom systemu na jednym aktywnym ekranie wyświetlacza. W przypadku systemów wieloużytkowych informacje muszą być dostępne dla każdego operatora systemu, który zostanie wyszczególniony jako właściciel alarmu (osoba, która aktywnie przetwarza alarm), a także dla operatora który aktualnie przegląda alarmy. Operatorzy ci muszą mieć możliwość korzystania z wbudowanej funkcji alarmu i notatki urządzenia, aby wysyłać notatki do siebie w czasie rzeczywistym lub zapisywać notatki, które operator systemu może wyświetlić w późniejszym czasie.

- **Nieograniczone konfigurowalne przepływy alarmów dla każdego typu alarmu**

- rozwiązanie musi umożliwiać operatorom systemu SMS, którzy mają właściwy poziom autoryzacji, na utworzenie szeregu procedur alarmowych które składają się w zestaw instrukcji lub czynności, które muszą być podjęte przez operatora systemu, zanim alarm może zostać zresetowany. Procedury pracy tzw. Workflow, raz utworzone, mogą być zapisywane dla pojedynczego alarmu lub zapisane jako szablon Workflow, który może być przypisany do każdego innego alarmu w celu ułatwienia konfiguracji. Po utworzeniu i przypisaniu Workflowów alarmowych muszą one być dostępne w aplikacji do przetwarzania alarmów.

- **Zaawansowana funkcja eskalacji alarmów z konfigurowalnymi strefami czasowymi**

- eskalacji alarmu to wymagana metoda, w której alarm może zwiększać priorytet z upływem czasu, gdy nie zostanie potwierdzony przez operatora systemu. Eskalacja alarmów musi być wysoce konfigurowalna, a alarmy o niskim prioryecie mogą być automatycznie eskalowane do wyższego poziomu priorytetu, jeśli nie zostaną potwierdzone w określonym czasie. Poziomy, na których alarm może wzrosnąć, mają mieć zdefiniowaną przez użytkownika wartość przyrostową. Reguły eskalacji alarmów mogą być stosowane w zależności od określonych typów alarmów, a także stref czasowych.

Okno eskalacji alarmu ma być wskazane przez system, tak aby tylko operatorzy z prawidłowym poziomem autoryzacji mogli oglądać eskalowane alarmy.

- **Baner priorytetu alarmu**

- system SMS musi posiadać dedykowany baner priorytetu alarmowego który zawsze wyświetla alarm o najwyższym priorytecie u góry ekranu, aby zapewnić, że najbardziej krytyczne alarmy systemowe są przetwarzane tak szybko, jak to możliwe. Każdy użytkownik ma możliwość skonfigurowania banera priorytetów alarmów, aby wyświetlać najpierw najnowsze lub najstarsze alarmy w oparciu o ich preferencje. Możliwe jest również dalsze skonfigurowanie banera alarmów, aby tylko najwyższe zdefiniowane przez użytkownika alarmy priorytetowe były wyświetlane w banerze priorytetu.

- **Akcje alarmowe**

- akcje alarmowe mają pozwolić operatorowi systemu z odpowiednim poziomem autoryzacji, aby skonfigurować i powiązać dowolny alarm systemowy z dowolnego typu urządzeniami i zainicjować aplikację innej firmy oraz przekazać parametry do tej aplikacji, jeśli jest to możliwe.

- **Graficzny wyświetlacz mapy w czasie rzeczywistym, który można dostosować do wymagań każdego operatora**

- aplikacja po skonfigurowaniu musi wyświetlać przyjazny dla użytkownika graficzny przegląd alarmów i urządzeń zawartych w systemie zarządzania bezpieczeństwem, szczegółowe informacje o urządzeniu, lokalizacji wejścia lub alarmu. Mapy muszą być dodawane do systemu w interfejsie opartym na drzewach, obejmującym przegląd budynku i mapy pięter. Każda mapa może być zagnieżdżona jedna na drugiej w nieograniczonej strukturze opartej na drzewach.

Mapy do systemu należy przesyłać w następujących formatach:

- .JPEG
- .PNG
- .BMP
- .GIF
- .TIF

Ikony urządzeń i dane wejściowe należy następnie przeciągnąć i upuścić na ich odpowiednie położenie w przesłanych mapach. Ikony muszą zostać dopasowane i skonfigurowane do określonego rozmiaru. Ponadto należy zdefiniować obszar powiadamiania o alarmie (obszar, który będzie wyświetlał migające wskazanie alarmu) każdego urządzenia lub ikony wejściowej.

- **Strefy mapy**

- system SMS musi pozwalać na narysowanie strefy w sekcji mapy poprzez dodanie punktów w żądanym obszarze, co z kolei tworzy linie. Każdą strefę można łatwo regulować, przesuwając

punkty strefowe i zmieniając kształt strefy. Urządzenia można wtedy umieszczać na mapach i w poszczególnych strefach.

- **Oneshot i broadcast do zdalnego otwierania i zarządzania drzwiami kontroli dostępu**

- system SMS musi zapewniać operatorom możliwość kontrolowania wszystkich urządzeń systemowych podłączonych do aplikacji. Operatorzy mogą otwierać kontrolowane drzwi bezpośrednio za pomocą ikon urządzeń, które można umieścić na mapach graficznych lub uruchomić z menu. Musi istnieć również możliwość wysyłania poleceń rozgłoszeniowych, które mogą otworzyć wszystkie lub grupę drzwi bezpośrednio z jednej zunifikowanej platformy bezpieczeństwa.

- **Dedykowane mikrokontrolery wideo do monitorowania alarmów w czasie rzeczywistym i archiwizacji**

- system SMS musi posiadać wbudowany podgląd wideo który pozwala aby operator bezpośrednio z poziomu systemu zarządzania bezpieczeństwem mógł wyświetlać na żywo i nagrany materiał filmowy jednocześnie przetwarzając alarmy w aplikacji przetwarzania alarmów. Podgląd wideo należy uruchomić za pośrednictwem karty wideo w obrębie systemu lub z wykorzystaniem powiązanego przetwarzania alarmów. Jeśli do alarmu przypisano więcej niż jedną kamerę lub urządzenie; musi być dostępna opcja wyboru każdego widoku z kamery, zarówno w przypadku nagrań, jak i na żywo, zgodnie z wymaganiami. Podgląd wideo wymaga systemu CCTV z pełną integracją z SMS.

- **Konfigurowalna ikona urządzenia i aplikacje zewnętrzne**

- funkcja aplikacji zewnętrznych musi pozwalać na dodawanie dowolnej aplikacji zewnętrznej do paska okna systemu; zapewnia to bezproblemowy interfejs niskopoziomowy dla dowolnego systemu innej firmy.

Możliwość uruchamiania aplikacji innych producentów bezpośrednio w SMS, zapewnia operatorom systemu szybki dostęp do kluczowych pakietów systemowych, które są wymagane do codziennej pracy systemu bezpieczeństwa. Na przykład HVAC, inteligentne oświetlenie, systemy wideo i CRM. Dodatkowo system musi umożliwiać tworzenie i umieszczanie ikon przycisków poleceń bezpośrednio na dowolnej mapie graficznej. Umożliwia to podgląd parametrów aplikacji i przekazywania ich w celu kontrolowania systemów innych producentów, takich jak oświetlenie, systemy HVAC i kontroli dostępu oraz systemy wideo, co ułatwia operatorom systemu kontrolowanie całego systemu zabezpieczeń i zarządzanie nim bezpośrednio z poziomu programu SMS.

- **Zaawansowane ograniczenia użytkowników dla aplikacji wielo-użytkownikowych, ograniczenie dostępu do map terenu, planów pięter, urządzeń i alarmów.**

- system SMS ma być zaprojektowany dla wielu użytkowników i musi mieć możliwość dostosowywania i ograniczania w zależności od konkretnych wymagań użytkownika. Aby to umożliwić, funkcje ograniczania użytkownika systemu SMS muszą umożliwiać administratorom tworzenie i przypisywanie szablonów ograniczeń użytkownika, które ograniczają dostęp do poszczególnych map obiektów, planów pięter, urządzeń, danych wejściowych, a także ograniczają

dostęp do wszystkich domyślnych i zdefiniowanych przez użytkownika alarmów systemu. Szablony te można następnie przypisać do konkretnych użytkowników, którzy zostali utworzeni w ramach platformy oprogramowania.

- **Dedykowane okno wyskakujące alarmu**

- aplikacja musi posiadać funkcję, w której na ekranie zostanie wyświetlone małe okno podręczne alarmu interaktywnego np. w sytuacjach, gdy operator przegląda inną aplikację poza aplikacją centrum bezpieczeństwa co gwarantuje, że operator nie przegapi żadnego alarmu w systemie bezpieczeństwa.

- **Wbudowane raporty systemowe dla szybkiego dostępu do alarmu, eskalacji alarmu i historii użytkownika**

- aplikacja musi oferować szeroką gamę raportów, które zawierają informacje o alarmach, eskalacji alarmów, priorytetach alarmów, użytkownikach, transakcjach urządzeń, śladach i numerach wersji. Każdy raport można skonfigurować i uruchomić na podstawie czasu i dat, urządzeń, priorytetów alarmowych, a nawet użytkowników. Każdy raport można wydrukować bezpośrednio z aplikacji bezpieczeństwa lub wyeksportować w formatach XPS lub PDF.

- **Poziom zagrożenia**

- system SMS musi umożliwiać operatorowi bezpieczeństwa przeglądanie i ustawianie poziomów zagrożenia bezpośrednio z poziomu aplikacji, a aktualny status ma być wyświetlany na głównym pasku stanu.

- **Funkcja Rolling Transaction Display (RTD)**

- funkcja Rolling Transaction Display (RTD), dostępna w systemie SMS musi pozwalać osobom odpowiedzialnym za bezpieczeństwo na bieżące śledzenie wszystkich transakcji oraz innych wydarzeń zachodzących w systemie kontroli dostępu. W ten sposób możliwa jest wizualna weryfikacja tożsamości użytkowników kart identyfikacyjnych, zanim umożliwi się im przejście przez określone drzwi. Za pośrednictwem aplikacji SMS należy uzyskać dostęp do funkcji RTD i wyświetlać ją za pomocą interfejsu użytkownika systemu SMS. RTD oferuje podzielony widok ekranu wyników transakcji i alarmów w systemie kontroli dostępu w czasie rzeczywistym, zapewniając pełną ścieżkę audytu transakcji widocznych w jednym oknie. RTD musi pozwalać operatorom wybrać, w jaki sposób chcą oglądać transakcje z opcjami dla "Prostej listy", "Listy szczegółów" lub "Listy obrazów", wraz z konfigurowalnymi efektami dźwiękowymi. Drzwi można otwierać za pomocą komendy "Oneshot", gdy operator zweryfikuje dostęp posiadacza karty.

- **W pełni zintegrowana funkcja śledzenia posiadaczy kart**

- aplikacja musi posiadać wbudowaną funkcję śledzenia posiadaczy kart, która pozwala operatorowi systemu podążać i śledzić każdego posiadacza karty, który został uznany jako zagrożenie lub istnieje prawdopodobieństwo, że będzie odpowiedzialny za bezpieczeństwo obiektu i osób w nim przebywających.

- **Zdarzenia i obchody strażnika**

- system SMS musi posiadać wbudowaną aplikację zdarzeń strażnika, która wyświetla wszystkie zdarzenia i powiadomienia o nadchodzącym obchodzie strażników. Informacje wyświetlane operatorowi systemu obejmują nazwę trasy wartowniczej, rodzaj zdarzenia, datę / godzinę, nazwę strażnika, adres urządzenia i opis wraz z aktywnym wejściem nadzoru straży. Obchody strażnicze mogą być konfigurowane, zarządzane i monitorowane bezpośrednio z poziomu aplikacji, zapewniając jednolity widok systemu zarządzania bezpieczeństwem.

· **Zarządzanie układem**

- system SMS musi zapewniać operatorom możliwość otwierania zestawu aplikacji i tworzenia ruchomych okien, które można następnie zgrupować w dostosowany układ ekranu w jednym lub wielu monitorowanych systemach. Dostosowane układy muszą być zapisywane w odniesieniu do użytkownika, a nie do stacji roboczej, co oznacza, że ten sam układ będzie przedstawiony operatorowi przy każdym logowaniu do stacji roboczej klienta. Układ należy skonfigurować tak, aby wyświetlał mapy, alarmy, wideo i przetwarzanie alarmów w układzie, który może poprawić ergonomię operatorów systemu.

· **Dostosowywanie aplikacji**

- system SMS ma być rozwiązaniem bardzo elastycznym i konfigurowalnym. SMS musi zapewniać operatorom możliwość korzystania z domyślnych ikon systemowych lub używania własnych niestandardowych ikon. Funkcjonalność dostosowywania programu SMS umożliwia operatorom określenie rozmiaru ikon, miejsca zakotwiczenia paska z ikonami, obszaru wyskakiwania alarmów, a także niestandardowego koloru dla każdego typu alarmu za pomocą zintegrowanej palety kolorów. Ustawienia te można następnie zapisać w szablonie urządzenia, który może być używany w innych konfiguracjach urządzeń w celu skrócenia czasu ustawiania. Wymagana jest także dodatkowa opcja, umożliwiająca konfigurowanie niestandardowych dźwięków dla każdego określonego typu alarmu, zgodnie z indywidualnymi preferencjami.

OPRACOWAŁ