GOREM Sp. z o.o.
ul. Wiślna 15
80-555 Gdańsk
Oddział w Gorzowie
ul. Przędzalnicza 16 ; 66-400 Gorzów Wlkp.

REMONT I PRZEBUDOWA BUDYNKU BIUROWEGO

działka nr ewid. 596/18; obręb 0010 Zamoście, ul. Targowa 9

jednostka ewidencyjna 086101_1 Miasto Gorzów Wielkopolski

województwo lubuskie, powiat Gorzów Wlkp.

TEMAT

PROJEKT WYKONAWCZY

NAZWA OPRACOWANIA

INSTALACJE TELETECHNICZNE LAN, KD, CCTV, SSWiN, SYSTEM PRZYWOŁAWCZY, ZASILANIE GWARANTOWANE

Gorzowski Ośrodek Technologiczny
Park Naukowo - Przemysłowy Sp. z o.o.
z siedzibą w Gorzowie Wlkp.
ul. Teatralna 49, 66-400 Gorzów Wlkp.

INWESTOR

PROJEKTANT IMIĘ I NAZWISKO	ZAKRES OPRACOWANIA	DATA	PODPIS	NR UPRAWNIEŃ
inż. Lech Kosobucki	Branża Elektryczna	VII-2020r.		52 / 84 w zakresie sieci i instalacji elektrycznych bez ograniczeń
OPRACOWAŁ Mgr inż. Franciszek Narkun	Branża Elektryczna	VII-2020r		Upr. bud. 11/89/Gw spec. inst. – inżynier. zakres sieci elektrycz.
KATEGORIA OBIEKTU: XVI ; XVII				NR EGZ. **/4**

Gorzów Wlkp. LIPIEC 2020r.

1 SPIS TREŚCI

2 SPIS RYSUNKÓW

L.P	Tytuł rysunku	Nr Rys.
1	SCHEMAT IDEOWY – LAN	T-01
2	WIDOK SZAF – GPD	T-02
3	RZUT PARTERU – LAN	T-03
4	RZUT I PIĘTRA – LAN	T-04
5	RZUT II PIĘTRA – LAN	T-05
6	RZUT III PIĘTRA – LAN	T-06
7	RZUT IV PIĘTRA – LAN	T-07
8	SCHEMAT INSTALACJI SYSTEMU PRZWOŁAWCZEGO	T-08
9	RZUT PARTERU– SYSTEM PRZYWOŁAWCZY	T-09
10	RZUT I PIĘTRA– SYSTEM PRZYWOŁAWCZY	T-10
11	RZUT II-III PIĘTRA– SYSTEM PRZYWOŁAWCZY	T-11
12	RZUT IV PIĘTRA– SYSTEM PRZYWOŁAWCZY	T-12
13	SCHEMAT INSTALACJI KD	T-13
14	SCHEMAT INSTALACJI CCTV	T-14
15	RZUT PARTERU – KD i CCTV	T-15
16	RZUT I PIĘTRA – KD i CCTV	T-16
17	RZUT II-III PIĘTRA – KD i CCTV	T-17
18	RZUT IV PIĘTRA – KD i CCTV	T-18
19		
20	SCHEMAT INSTALACJI SSWiN	T-20
21	RZUT PARTERU – SSWiN	T-21
22	RZUT I PIĘTRA – SSWiN	T-12
23	RZUT II-III PIĘTRA – SSWiN	T-23
24	RZUT IV PIĘTRA – SSWiN	T-24
24	RZUT DACHU – SSWiN	T-25
26	SCHEMAT ROZDZIELNICY TI+TLK	T-26
27	SCHEMAT ROZDZIELNICY TLK	T-26A
28	SCHEMAT ROZDZIELNICY TUK	T-27
29	SCHEMAT ROZDZIELNICY TBK3	T-28
30	SCHEMAT ROZDZIELNICY TBK2	T-29

3 ZAKRES PROJEKTU

Przedmiotem niniejszego opracowania jest projekt instalacji okablowania strukturalnego, urządzeń aktywnych, systemu CCTV, systemu KD, systemu przywoławczego systemu sygnalizacji włamania i napadu oraz instalacji zasilania gwarantowanego instalacji LAN. Opracowanie to dotyczy remontu i przebudowy budynku biurowego przy ul. Targowej 9 w Gorzowie Wielkopolskim 66-400, zlokalizowanego na działce 596/18, obr. Zamoście.

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.

Projekt opisuje minimalne wymagania użytkownika w zakresie technicznym i funkcjonalnym. Oznacza to, że zgodnie z warunkami ustawy Prawo Zamówień Publicznych, można zastosować dowolne rozwiązanie spełniające wszystkie kryteria opisane w dokumentacji projektowej, tj. zgodne pod kątem obowiązującej normalizacji, wymaganych parametrów oraz funkcji. Składając ofertę, wykonawca ma przedstawić nazwę producenta oraz listę materiałów w formie tabeli, zawierającej nr katalogowy producenta, nazwę produktu oraz zaplanowaną ilość - w celu zapewnienia możliwości weryfikacji wszystkich wymaganych parametrów technicznych oraz funkcji użytkowych.

4 INSTALACJA LAN

4.1 Podstawa opracowania projektu

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

Środowisko najbardziej zbliżone do środowiska biurowego. 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.
- PN-EN 50310:2016 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym.

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.

4.2 Wymagania ogólne dotyczące okablowania strukturalnego

- okablowanie strukturalne budowane jest, zgodnie z w/w normami, tj. w konfiguracji gwiazdy/gwiazdy hierarchicznej i przy rygorze, że łącza stałe nie mogą przekroczyć długości 90 m;
- 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;
- ilość i rozmieszczenie stanowisk roboczych 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;
- wszystkie elementy pasywne składające się na okablowanie strukturalne muszą być trwale oznaczone nazwą lub znakiem firmowym tego samego producenta-wytwórcy elementów okablowania i pochodzić z jednolitej oferty kompletnego systemu w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu gwarancyjnego w/w producenta-wytwórcy;
- maksymalna długość kabla instalacyjnego (od punktu dystrybucyjnego do gniazda końcowego) nie może przekroczyć 90 metrów;
- minimalne wymagania elementów okablowania w systemie zamkniętym dla transmisji danych pod względem wydajności to Kategoria 6_A (komponenty)/ Klasa E_A (podstawowa wydajność całego systemu) i zapewnienie możliwości transmisji 10Gigabit Ethernet 802.3an oraz docelowa wydajność kanału transmisyjnego zbudowanego z kabli miedzianych to Klasa E_A;
- okablowanie w budynku obsługiwane jest przez Główny Punkt Dystrybucyjny GPD zlokalizowany w pomieszczeniu 1.02 (Serwerownia zlokalizowana na I piętrze), składający się z dwóch szaf serwerowych 42U o wymiarach 800x800 mm;
- punkt dystrybucyjny jest zlokalizowany w zaznaczonym na rzutach pomieszczeniu na I piętrze, ewentualne zmiany lokalizacji mają być uwzględnione na etapie wykonawczym oraz zaznaczone w dokumentacji powykonawczej;
- okablowanie strukturalne wewnątrz budynku ma być prowadzone podwójnie ekranowanym kablem typu F/FTP kat. 6_A o paśmie przenoszenia 500 MHz w osłonie trudnopalnej typu LSZH;
- osłona zewnętrzna kabla w okablowaniu poziomym oraz szkieletowym ma być trudnopalna i niewydzielająca trujących substancji w obecności ognia. Osłona kabli miedzianych ma posiadać czynnik opóźniający rozprzestrzenianie się ognia;
- wszystkie kable okablowania poziomego mają być zakończone w osprzęcie połączeniowym zgodnie z normą PN-EN 50173-1;
- aby zagwarantować i potwierdzić wymaganą wydajność komponentów okablowania miedzianego przeznaczonych do zabudowy (kabel oraz gniazdo) producent musi posiadać certyfikaty wydane przez akredytowane niezależne laboratoria (np. GHMT, Delta) potwierdzające zgodność systemu / komponentów z wymaganiami normy międzynarodowej, tj. ISO/IEC 11801 lub EN50173-1 do minimum klasy E_A;

- punkty końcowe użytkownika mają składać się z gniazd w systemie zamkniętym według schematu ideowego okablowania;
- okablowanie ma być realizowane poprzez ekranowane moduły gniazd RJ45 kat. 6_A składające się z dwóch elementów, posiadających zacisk ekranu kabla (360^o), dla kamer zewnętrznych poprzez ekranowane wtyki RJ45 kat. 6_A;
- dla systemu ekranowanego należy zastosować proste panele krosowe o wysokości 1U, niezaładowane, na 24 oddzielne moduły ekranowane;
- punkty końcowe systemu oparte zostały na ekranowanym gnieździe teleinformatycznym w uchwycie do osprzętu 45x45;
- nie dopuszcza się stosowania gniazd i wtyków z niestandardowymi interfejsami (takimi, do których nie ma referencji w dokumentach z Rozdziału 4.1).
- operator usług teleinformatycznych musi doprowadzić połączenie między przyłączem telekomunikacyjnym a szafami w serwerowni.

4.3 Trasy kablowe

4.3.1 **Okablowanie szkieletowe**

Okablowanie szkieletowe występuje na odcinku między przyłączem telekomunikacyjnym, a szafą GPD zlokalizowaną w pomieszczeniu 1.02. ma zostać zapewnione przez operatora usług teleinformatycznych.

4.3.2 **Prowadzenie okablowania w pionach kablowych**

Trasy kablowe – pionowe należy zbudować z drabinek pozwalających na zamocowanie kabli oraz zachowanie odpowiednich promieni gięcia wiązek kablowych na zakrętach. W przypadku przebić/przejść pomiędzy kondygnacjami nie realizowanymi w szachtach teleinformatycznych, należy zastosować zabezpieczenie zgodne z zasadami p.poż..

4.3.3 **Prowadzenie okablowania poziomego**

Okablowanie poziome zostanie rozprowadzone:

- trasy kablowe należy prowadzić w przestrzeniach nad sufitem podwieszanym, podtynkowo w rurach elektro-instalacyjnych typu peszel oraz w korytach podłogowych;
- główne ciągi kablowe wzdłuż korytarza oraz w pomieszczeniach w nowo projektowanych korytach kablowych 50x50, 60x200, 60x300 zgodnie z podkładami;
- dopuszcza się mocowanie okablowania za pomocą opasek kablowych spinających maksymalnie 24 kable w jednej wiązce;
- w celu zabezpieczenia kabli przed nadmiernymi naprężeniami w szachtach należy zastosować drabinki kablowe, do których należy przymocować kable za pomocą opasek kablowych;
- w pomieszczeniach do punktu logicznego w nowo projektowane trasy kablowe należy prowadzić podtynkowo w rurach elektro-instalacyjnych typu peszel, w przestrzeni nad sufitem podwieszanym lub w korytach podłogowych;
- średnicę rury elektro-instalacyjnej należy dobrać do średnicy i ilości kabli zachowując promienie gięcia zalecane dopuszczalne przez producenta okablowania;
- w pomieszczeniu serwerowni na I piętrze w nowo projektowanych korytach kablowych 2x 60x300;
- przejścia tras kablowych między strefami pożarowymi należy zabezpieczyć przed rozprzestrzenianiem się ognia masą ognioodporną.
- Zasilanie elektryczne instalacji LAN prowadzić w oddzielnych kotytkach nad sufitem podwieszanym w korytyarzu

Budowa tras kablowych ma zapewniać łatwe, bezkolizyjne i bezpieczne prowadzenie kabli uwzględniając inne instalacje w budynku.

4.3.4 **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. Obliczone wartości separacji dla kabli wybranych w projekcie od kabli zasilających:

- w korytarzach koryta okablowania strukturalnego mają być odseparowane od koryt, w których prowadzone są kable elektryczne na odległość minimum 1cm;
- w pomieszczeniach użytkowych minimum 0,2 cm od kabli zasilających.

4.4 Okablowanie poziome

Kable okablowania poziomego mają być zakończone w zestawach gniazd, zwanych dalej punktami logicznymi (PL), punktami elektryczno–logicznymi (PEL), wtykami RJ45. Zestawy gniazd mają być zgodne ze standardem uchwytu osprzętu elektroinstalacyjnego 45x45. Gniazda mają być montowane podtynkowo oraz podłogowo, w puszkach w uchwycie montażowym 45x45 w ilościach w zależności od konfiguracji PL lub PEL. Ostateczna lokalizacja powinna być ustalona z Użytkownikiem.

4.4.1 **Punkt Logiczny PL1 - CCTV, KD**

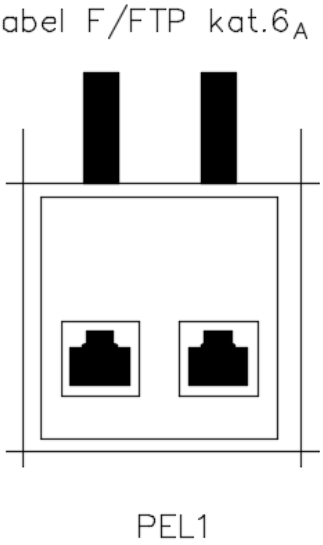
Konfiguracja: Gniazda PL1 będą instalowane w pomieszczeniach zgodnie z podkładami budowlanymi. Do PL1 doprowadzić 1 kabel F/FTP kat. 6_A, który należy zakończyć zamontowanym ekranowanym modułem teleinformatycznym RJ45 kat.6_A.

4.4.2 **Punkt Logiczny PL2 - WiFi**

Konfiguracja: Gniazda PL2 będą instalowane w pomieszczeniach zgodnie z podkładami budowlanymi. Do PL2 doprowadzić 2 kable F/FTP kat. 6_A, które należy zakończyć dwoma zamontowanymi ekranowanymi modułami teleinformatycznymi RJ45 kat.$6_{A.}$

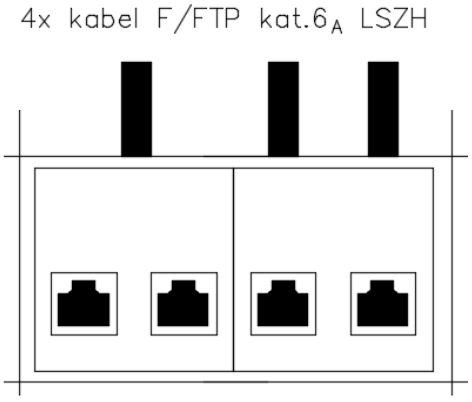
4.4.3 **Punkt Elektryczno-Logiczny PEL1 - LAN**

Konfiguracja: Gniazda PEL1 będą instalowane w pomieszczeniach zgodnie z podkładami budowlanymi. Do PEL1 doprowadzić 2 kable F/FTP kat. 6_A, które należy zakończyć dwoma zamontowanymi ekranowanymi modułami teleinformatycznymi RJ45 kat.6_A. i 3 gniazda 230V czerwone z kluczem



4.4.4 **Punkt Elektryczno-Logiczny PEL2 - LAN**

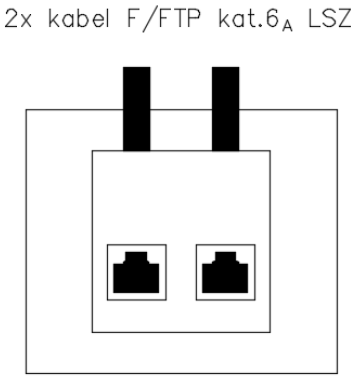
Konfiguracja: Gniazda PEL2 będą instalowane w pomieszczeniach zgodnie z podkładami budowlanymi. Do PEL2 doprowadzić 4 kable F/FTP kat. 6_A, które należy zakończyć czterema zamontowanymi ekranowanymi modułami teleinformatycznymi RJ45 kat.6_A. i 3 gniazda 230V czerwone z kluczem



PEL2

4.4.5 **Punkt Elektryczno-Logiczny PEL3 - LAN**

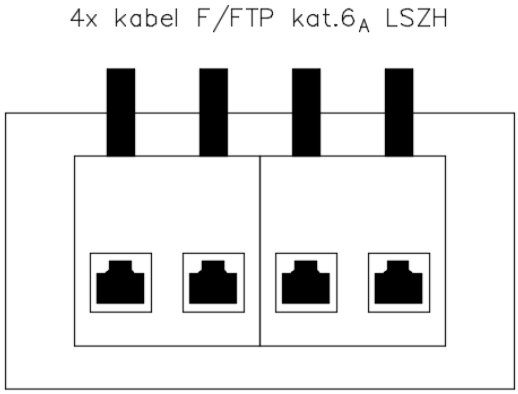
Konfiguracja: Gniazda PEL3 będą instalowane w pomieszczeniach zgodnie z podkładami budowlanymi. Do PEL3 doprowadzić 2 kable F/FTP kat. 6_A, które należy zakończyć dwoma zamontowanymi ekranowanymi modułami teleinformatycznymi RJ45 kat.6_A. i 3 gniazda 230V czerwone z kluczem Gniazda zasilające mogą być umieszczone z obu stron gniazd PEL3. Gniazda PEL3 mają być montowane w puszkach podłogowych.



PEL3

4.4.6 **Punkt Elektryczno-Logiczny PEL4 - LAN**

Konfiguracja: Gniazda PEL4 będą instalowane w pomieszczeniach zgodnie z podkładami budowlanymi. Do PEL4 doprowadzić 4 kable F/FTP kat. 6_A, które należy zakończyć czterema zamontowanymi ekranowanymi modułami teleinformatycznymi RJ45 kat.6_A. Gniazda zasilające mogą być umieszczone z obu stron gniazd PEL4. i 3 gniazda 230V czerwone z kluczem Gniazda PEL4 mają być montowane w puszkach podłogowych.



4.5 Wymagania dla kabli symetrycznych

Należy stosować kable w powłokach LSZH. Przy prowadzeniu tras kablowych zachować bezpieczne odległości od innych instalacji. W przypadku traktów, gdzie kable sieci teleinformatycznej i zasilającej biegną razem i równolegle do siebie, należy zachować odległość (rozdział) między instalacjami (szczególnie zasilającą i logiczną), co najmniej 10 mm lub stosować metalowe przegrody. Wielkość separacji dla trasy kablowej jest obliczona dla przypadku kabli F/FTP kat. 6_A.

Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 7,0 mm (co determinuje maksymalną średnicę żyły na 23AWG). Nie dopuszcza się kabli o większej średnicy zewnętrznej.

Instalacja ma być poprowadzona ekranowanym kablem konstrukcji F/FTP z osłoną zewnętrzną 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 miedzy parami),
2) w postaci jednostronnie laminowanej folii aluminiowej oplatającej 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.

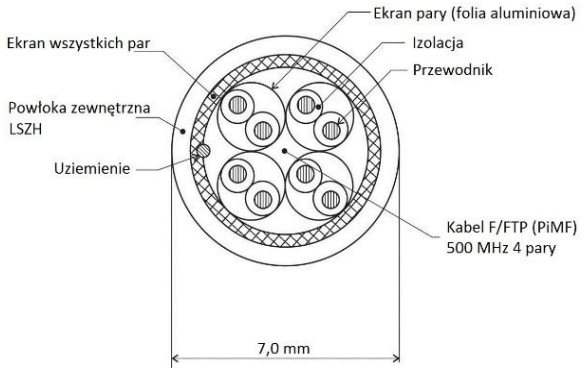
Charakterystyka kabla ma uwzględniać odpowiedni margines pracy, tj. pozytywne parametry transmisyjne do min. 500 MHz dla kabla kat.6_A.

W celu zagwarantowania najwyższej jakości połączenia przede wszystkim powtarzalnych parametrów, wszystkie złącza, zarówno w gniazdach końcowych jak i panelach muszą być zarabiane za pomocą standardowych narzędzi instalacyjnych. 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 6_A przez obowiązujące specyfikacje norm, równocześnie zapewniając pełną zgodność z niższymi kategoriami okablowania.

Tabela 1. Wymagania dla kabla (F/FTP kat.6_A)

Budowa kabla	F/FTP (zgodnie z rysunkiem)
Wydajność kabla	Kategoria 6_A wg. ISO/IEC 11801; EN 50173-1 500MHz
Certyfikat	Producent musi dostarczyć certyfikat wydany przez laboratorium potwierdzający jego charakterystyki na kategorię 6_A
Normy dotyczące palności	IEC 60332-1, IEC 60754-1, IEC 60754-2, IEC 61034-2
Tłumienie sprzężenia	Min. 41,3dB
Średnica zewnętrzna kabla	max.7,0 mm
Średnica żyły	23AWG (Φ 0.54 – 0.61mm)
Waga	47,0 – 49,0 kg/km
Temperatura podczas instalacji	Minimum przedział 0ºC do +50ºC
Osłona zewnętrzna	LSZH



Rys. 6. Budowa kabla kat. 6_A F/FTP

Tabela 2. Wymagania dla parametrów transmisyjnych kabla przy częstotliwościach kluczowych

Częstotliwość	**Tłumienie**	**PSNEXT**	**RL**
[MHz]	[dB]	[dB]	[dB]
300	31,8	94,6	27,7
500	41,3	91,6	26,9

4.6 Wymagania dotyczące gniazd

Wszystkie gniazda mają być zakańczane za pomocą narzędzi, które pozwalają zakończyć wszystkie pary w jednym ruchu i z jednakową siłą. Celem jest zachowanie minimalnego rozplotu par nie większego niż 6 mm 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 6_A do 500 MHz dla wszystkich

gniazd kat. 6_A przeznaczonych do zabudowy zgodnie ze specyfikacją PN-EN 50173-1 lub ISO/IEC11801.

Obudowa gniazda ma się składać w szczelną elektromagnetycznie całość, tworzącą klatkę Faradaya. Kabel ma być zamontowany w gnieździe w taki sposób aby był zapewniony styk elektryczny ekranu kabla z obudową gniazda na całym jego obwodzie.

4.7 Wymagania dotyczące paneli krosowych

Kable miedziane okablowania poziomego należy zakończyć na panelach krosowych niezaładowanych prostych o wysokości montażowej 1U i pojemności do 24 gniazd. Każdy port ma mieć możliwość oddzielnego opisu i oznaczenia poprzez system jednolitych oznaczeń. Panel ma być wyposażony w tylny wspornik w celu ułożenia i zamocowania do niego kabli, oraz zacisk uziemiający.

Panele mają być wyposażone w takie same moduły RJ45 co w punktach dostępowych użytkownika (punktach logicznych).

4.8 Kable krosowe miedziane

Kable obszaru roboczego (przyłączane do stacji użytkownika), jak i krosowe (w szafie kablowej) mają być wykonane kablem ekranowanym S/FTP 500 MHz. 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. Dodatkowo kable krosowe miedziane mają być zgodne ze specyfikacją kat.6_A. Wymagane jest, aby były wykonane fabrycznie ekranowanym kablem krosowym S/FTP 500 MHz, posiadające osłonę LSZH.

4.9 Punkty dystrybucyjne

4.9.1 **Szafy dystrybucyjne**

W szafach dystrybucyjnych należy zainstalować osprzęt połączeniowy oraz sprzęt aktywny.

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

Uwaga:

Lokalizacja szaf w budynku została pokazana na podkładach dołączonych do projektu i pokazana na schemacie ideowym okablowania strukturalnego.

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

Sprzęt należy instalować zgodnie z rozmieszczeniem przedstawionym na rysunkach dołączonych do projektu. Okablowanie poziome oraz szkieletowe należy wprowadzać do szaf od dołu, przez przepust szczotkowy umieszczony w cokole lub od góry poprzez otwór powstały przez wyciągnięcie dekla 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.

Wymagane właściwości dla szafy dystrybucyjnej GPD.1 i GPD.2:

- wysokość 42U, szerokość 800 mm oraz głębokość 800 mm;
- drzwi przednie i tylnie dwuskrzydłowe z perforacją;
- ściany boczne i tylna zdejmowane;
- perforacja u dołu szafy na wszystkich ścianach;
- „belki poziome" mocowane do zewnętrznego stelaża szafy po 2 z każdej strony przeznaczone do mocowania kabli skrętkowych, z możliwością instalacji dodatkowych belek;
- 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 zaślepiającymi otwory do wprowadzenia kabli od dołu;
- otwór o wysokości min. 3U i szerokości min 450 mm znajdujące się w dolnej części tylnej ściany szafy;
- szafa ma posiadać nóżki regulowane lub możliwość zastosowania kół jezdnych;
- szafa musi być wypoziomowana.

4.10 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 powtórną instalacją wadliwych elementów);
- ma obejmować całość okablowania miedzianego wraz z kablami krosowymi i innymi elementami niezbędnymi do budowy sieci takimi jak panele krosowe, gniazda RJ45, wieszaki 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.

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 łączy 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, funkcjonal-

nym oraz estetycznym. Użytkownik/Inwestor musi otrzymać raport, potwierdzający sprawdzenie instalacji oraz ma prawo uczestniczyć w procesie jej weryfikacji.

Obowiązki instalatora

Wykonawca ma posiadać aktualną umowę zawartą bezpośrednio z producentem okablowania regulującą uprawnienia, procedury, warunki i tryb udzielenia gwarancji Użytkownikowi.

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, osoby te muszą uczestniczyć w nadzorze zadania lub być na każde wezwanie na etapie realizacji.

Powyższe kursy mają znajdywać się w oficjalnej ofercie producenta.

Dokumenty mają być przedstawione Zamawiającemu przed podpisaniem umowy.

Dostarczone elementy pasywne (kable miedziane, panele krosowe, kable krosowe itp.) 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.

4.11 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.

4.12 Odbiór i pomiary sieci

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 powinno być zgodne z normą PN-EN 50697:2019-08. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego.

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 informacja 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.

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);
- pomiary dla systemu należy wykonać w konfiguracji pomiarowej kanału (Channel) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego;
- pomiary sieci miedzianej należy wykonać na zgodność z ISO/IEC11801 lub EN 50173-1:
  - klasa E_A dla wszystkich torów transmisyjnych;
- protokół pomiarowy każdego toru transmisyjnego poziomego miedzianego ma zawierać:
  - mapę połączeń;
  - długość połączeń i rezystancje par;
  - opóźnienie propagacji oraz różnicę opóźnień propagacji;
  - tłumienie;
  - NEXT i PS NEXT w dwóch kierunkach;
  - ACR-F i PS ACR-F w dwóch kierunkach;
  - ACR-N i PS ACR-N w dwóch kierunkach;
  - RL w dwóch kierunkach.

Zawartość dokumentacji powykonawczej

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

- raporty z pomiarów dynamicznych okablowania;
- rzeczywiste trasy prowadzenia kabli;
- rysunki z oznaczeniami poszczególnych szaf, paneli krosowych i portów;
- lokalizację przebić przez ściany i podłogi.

4.13 Uwagi końcowe

Trasy prowadzenia okablowania poziomego zostały skoordynowane 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.

Jeżeli oferent zdecyduje się na zastosowanie rozwiązania alternatywnego, powinien do oferty dołączyć listę zamienionych materiałów, jak również wszelkie dokumenty pozwalającej Komisji Przetargowej ocenić zgodność z wymaganiami SIWZ i dokumentacji projektowej wraz z załącznikami.

5 URZĄDZENIA AKTYWNE

5.1 Założenia ogólne

SIEĆ DOSTĘPOWA LAN

Projektowane urządzenia aktywne mają zapewniać niezawodną transmisję protokołu IEEE 1000Base-T oraz automatycznego przełączania do niższych prędkości (np. IEEE 100Base-T) dla połączeń z urządzeniami końcowymi w sieci poziomej wykorzystując jako medium skrętkę miedzianą FTP. Urządzenia aktywne mają być wyposażone w odpowiednie wymienne moduły światłowodowe zapewniające transmisję pomiędzy poszczególnymi węzłami sieci w zależności od faktycznych odległości toru światłowodowego.

W ramach GPD zainstalowane zostaną przełączniki sieciowe agregujące ruch z wszystkich punktów elektryczno-logicznych (PEL) rozmieszczonych w budynku. Dla ułatwienia procesów zarządzania oraz zwiększenia bezpieczeństwa i wydajności instalacji, w sieci aktywnej zostaną wydzielone następujące grupy funkcyjne (podsieci):

- sieć LAN – komputery użytkowników końcowych,
- sieć WiFi – punkty dostępowe i kontroler oraz użytkownicy sieci bezprzewodowej WLAN,
- sieć CCTV – kamery dozoru wizyjnego (wewnętrzne i zewnętrzne),
- sieć KD – elementy aktywne sieci kontroli dostępu fizycznego.

Sieć aktywna zostanie oparta na urządzeniach dostępowych wyposażonych w adekwatną do liczby gniazd (PEL) liczbę portów dostępowych. Urządzenia aktywne zostaną zainstalowane w szafie teletechnicznej typu Rack 19” w GPD, co ma zapewnić połączenia na odległości nie większe niż 90 m w torze kablowym. W ramach GPD planuje się zainstalowanie odpowiedniej liczby przełączników wyposażonych w 24 lub 48 interfejsów dostępowych w standardzie 100/1000Base-T RJ45. Dla potrzeb połączeń urządzeń dostępowych wymagających zasilania niskoprądowego (kamery CCTV i punkty dostępowe sieci WLAN) planuje się zastosowanie urządzeń wpierających technologię Power over Ethernet (PoE) zgodnie ze standardami IEEE 802.3af (PoE) oraz IEEE 802.3at (PoE+) zapewniających budżet mocy PoE 740W dla przełącznika 48-portowego oraz 380W w przypadku przełącznika 24-portowego z możliwością dostarczenia min. 15W na każdym porcie dostępowym jednocześnie.

Poniższa tabela przedstawia wymaganą liczbę portów 100/1000Base-T RJ45 dla każdego z poziomów wraz z podziałem na poszczególne grupy funkcyjne:

Tabela 3. Liczba punktów elektryczno-logicznych sieci aktywnej

POZIOM / SIEĆ	parter	I piętro	II piętro	III piętro	IV piętro	SUMA/SIEĆ

Sieć LAN	42	100	140	140	92	514
Sieć WiFi (PoE)	10	10	10	10	10	50
Sieć CCTV (PoE)	9	6	4	4	4	27
Sieć KD	1	5				6
SUMA/POZIOM	62	121	154	154	106	

Na potrzeby przyszłej rozbudowy projektuje się wyposażenie każdej z grup funkcyjnych w urządzenia aktywne zapewniające odpowiednią liczbę portów dostępowych zgodnie z poniższym zestawieniem sprzętowym:

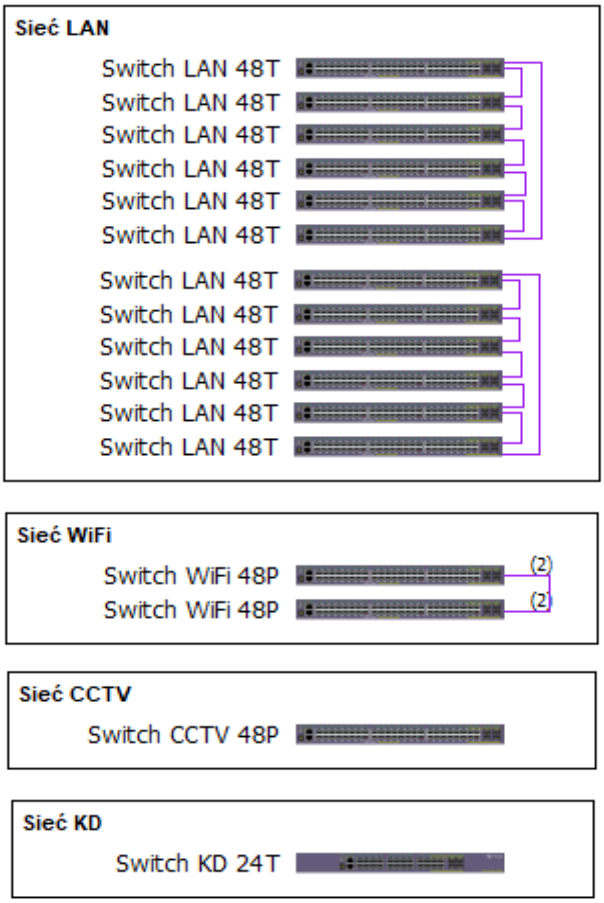
Tabela 4. Wyposażenie przełączników sieci aktywnej

POZIOM / SIEĆ	Switch 48T	Switch 48P (PoE)	Switch 24T	Projektowana liczba portów
Sieć LAN	12			576
Sieć WiFi (PoE)		2		96
Sieć CCTV (PoE)		1		48
Sieć KD			1	24
SUMA	12	3	1	744

Poszczególne podsieci będą realizowane z wykorzystaniem odrębnych urządzeń aktywnych co zapewni wysoką niezawodność i odpowiedni poziom przepustowości dla każdej podsieci. Urządzenia aktywne zostaną połączone w stosy – połączenie fizycznych przełączników w zarządzane z pojedynczego adresu IP jedno logiczne urządzenie. Do łączenia przełączników zostaną wykorzystane dedykowane interfejsy – bez ograniczania liczby interfejsów dostępowych oraz uplink. Architektura stosu będzie umożliwiać realizację zamkniętej pętli dla zapewnienia redundancji. Wydajność przełączania w stosie wynosić będzie 40Gbps. Możliwe będzie połączenie do 8 przełączników w stos. Stos przełączników może składać się z urządzeń 48-portowych w wersji z PoE lub bez. Wszystkie przełączniki w ramach stosu pochodzić będą od tego samego producenta. Możliwości rozbudowy stosu nie będą ograniczone do stosowania urządzeń pochodzących z tej samej serii – na potrzeby rozbudowy o dodatkowe porty światłowodowe dla urządzeń których odległość jest większa niż 90 m lub opóźnienia w transmisji wymagają połączeń światłowodowych.

5.2 Schemat podziału sieci aktywnej

Poniższy rysunek przedstawia schemat podziału sieci aktywnej na grupy funkcyjne:



Rysunek 7. Podział sieci aktywnej wraz z zestawieniem urządzeń

5.3 Wymagania szczegółowe dla poszczególnych komponentów sieciowych – urządzeń sieciowych zastosowanych w ramach niniejszego projektu

Przestawione we wcześniejszej części opisu komponenty sieciowe, zostały przedstawione szczegółowo poniżej, w ramach odpowiednich rozdziałów. Przedstawione zakresy są zakresami minimalnymi do spełnienia, w umożliwienia na etapie realizacji funkcjonalności wymaga-nych w ramach wdrażanych systemów i aplikacji wykorzystywanych na obiekcie. Poniżej znajdują się głównie komponenty sprzętowe, dane techniczne i funkcjonalne urządzeń sieciowych wymagane do zastosowania.

5.3.1 Przełącznik CCTV

Wymagania podstawowe

1. Przełącznik posiadający min. 48 interfejsów 10/100/1000BASE-T RJ45, min. 4 interfejsy 1GBASE-X SFP oraz 2 interfejsy 10GBASE-X SFP+ do łączenia urządzeń w stos.
2. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management.

3. Przełącznik musi wspierać technologię Power over Ethernet (PoE) zgodnie ze standardami IEEE 802.3af (PoE) oraz IEEE 802.3at (PoE+) do zasilania urządzeń takich jak punkty dostępowe WLAN, telefony VoIP i kamery monitoringu wizyjnego.
4. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich interfejsach 10/100/1000BASE-T.
5. Wysokość urządzenia nie więcej niż 1U.
6. Przełącznik musi posiadać wbudowany zasilacz 230V AC zapewniający budżet mocy dla technologii PoE na poziomie min. 740W zapewniając jednocześnie min. 15W dla wszystkich interfejsów 10/100/100BASE-T.
7. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
8. Przełącznik musi posiadać nieblokującą architekturę o wydajności przełączania min. 176 Gbps oraz szybkości przełączania min. 130 Mpps.
9. Musi posiadać możliwość realizacji stosów – łączenia fizycznych przełączników w zarządzane z pojedynczego adresu IP jedno logiczne urządzenie. Do łączenia przełączników muszą być wykorzystane dedykowane interfejsy – bez ograniczania liczby interfejsów uplink. Architektura stosu musi umożliwiać realizację zamkniętej pętli. Wydajność przełączania w stosie min. 40Gbps. Wymagana jest możliwość łączenia do 8 przełączników w stos (w tym również przełączników nie wspierających technologii PoE).
10. Tablica MAC adresów min. 16k.
11. Pamięć operacyjna: min. 1GB pamięci DRAM.
12. Pamięć flash: min. 2GB pamięci Flash.
13. Pojemność bufora pakietów min. 1,5 MB.
14. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
15. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
16. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów).
17. Obsługa Q-in-Q IEEE 802.1ad.
18. Obsługa Quality of Service:
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
19. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
20. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) .
21. Wbudowany DHCP serwer i klient.
22. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
23. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci.
24. Możliwość monitorowania zajętości CPU.
25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)

Obsługa routingu IPv4

26. Sprzętowa obsługa routingu IPv4 – forwarding.
27. Pojemność tabeli routingu min. 450 wpisów.
28. Routing statyczny.
29. Obsługa routingu dynamicznego IPv4 ze wsparciem przynajmniej dla protokołu RIPv1/v2.
30. Policy Based Routing dla IPv4.
31. Obsługa DHCP/BootP Relay dla IPv4

32. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF.

Obsługa routingu IPv6

33. Sprzętowa obsługa routingu IPv6 – forwarding.
34. Pojemność tabeli routingu min. 225 wpisów.
35. Routing statyczny.
36. Obsługa routingu dynamicznego dla IPv6 ze wsparciem przynajmniej dla protokołu RIPng.
37. Policy Based Routing dla IPv6.
38. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF v3.

Obsługa ruchu multicast

39. Statyczne przyłączenie do grupy multicast
40. Filtrowanie IGMP
41. Obsługa Multicast VLAN Registration - MVR
42. Obsługa IGMP v1/v2/v3
43. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo sieciowe

44. Obsługa uwierzytelniania stacji roboczych z wykorzystaniem mechanizmów:
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
45. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants)
46. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
47. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC
48. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
49. Urządzenie musi wspierać profile bezpieczeństwa, profil bezpieczeństwa oznacza połączenie:
    a. definicji sieci VLAN,
    b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
    c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
    d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
50. Obsługa Guest VLAN dla IEEE 802.1x
51. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
52. Wbudowana obrona procesora urządzenia przed atakami DoS
53. Obsługa TACACS+ (RFC 1492)
54. Obsługa RADIUS Authentication (RFC 2865)
55. Obsługa RADIUS Accounting (RFC 2866)
56. RADIUS and TACACS+ per-command Authentication
57. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
58. Możliwość wyłączenia MAC learning
59. Obsługa SNMPv1/v2/v3

60. Klient SSH2
61. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
62. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
63. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
64. Obsługa bezpiecznego transferu plików SCP/SFTP
65. Obsługa DHCP Option 82
66. Obsługa Gratuitous ARP Protection
67. Obsługa Trusted DHCP Server
68. Obsługa DHCP Snooping
69. Obsługa DHCP Secured ARP/ARP Validation
70. Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x
71. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s
72. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
73. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
74. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
75. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
76. Obsługa PVST+
77. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
78. Obsługa G.8032
79. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
80. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

81. Obsługa synchronizacji czasu NTP lub SNTP
82. Zarządzanie przez SNMP v1/v2/v3
83. Zarządzanie przez przeglądarkę WWW – protokół http i https
84. Telnet Serwer/Klient dla IPv4 / IPv6
85. SSH2 Serwer/Klient dla IPv4 / IPv6
86. Ping dla IPv4 / IPv6
87. Traceroute dla IPv4 / IPv6
88. Obsługa SYSLOG z możliwością definiowania wielu serwerów
89. Sprzętowa obsługa NetFlow lub sFlow
90. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
91. Obsługa RMON2 (RFC 2021)

Inne

92. Obsługa skryptów CLI
93. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
94. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu

c. Na podstawie wpisów w logu systemowym

Gwarancja

95. Wraz z urządzeniem wymagane jest dostarczenie kontraktu serwisowego na okres min. 1 roku umożliwiającego:
    a. bezpłatne aktualizacje oprogramowania firmware,
    b. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego od zgłoszenia awarii,
    c. wsparcia technicznego producenta poprzez infolinię, pocztę e-mail oraz telefon.

Wyposażenie dodatkowe

96. Wraz z każdym przełącznikiem należy dostarczyć:
    a. niezbędne okablowanie zasilające 230VAC,

5.3.2 Przełącznik KD

Wymagania podstawowe

1. Przełącznik posiadający min. 24 interfejsy 10/100/1000BASE-T RJ45, min. 4 interfejsy 1GBASE-X SFP oraz 2 interfejsy 10GBASE-X SFP+ do łączenia urządzeń w stos.
2. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
3. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T.
4. Wysokość urządzenia 1U.
5. Przełącznik musi posiadać wbudowany zasilacz 230V AC.
6. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
7. Przełącznik musi posiadać nieblokującą architekturę o wydajności przełączania min. 128 Gbps oraz szybkości przełączania min. 95 Mpps.
8. Musi posiadać możliwość realizacji stosów – łączenia fizycznych przełączników w zarządzane z pojedynczego adresu IP jedno logiczne urządzenie. Do łączenia przełączników muszą być wykorzystane dedykowane interfejsy – bez ograniczania liczby interfejsów uplink. Architektura stosu musi umożliwiać realizację zamkniętej pętli. Wydajność przełączania w stosie min. 40Gbps. Wymagana jest możliwość łączenia do 8 przełączników w stos (w tym również przełączników wspierających technologię PoE).
9. Tablica MAC adresów min. 16k.
10. Pamięć operacyjna: min. 1GB pamięci DRAM.
11. Pamięć flash: min. 2GB pamięci Flash.
12. Pojemność bufora pakietów min. 1,5 MB.
13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
14. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
15. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów).
16. Obsługa Q-in-Q IEEE 802.1ad.
17. Obsługa Quality of Service:
    a. IEEE 802.1p

    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
18. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
19. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) .
20. Wbudowany DHCP serwer i klient.
21. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
22. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci.
23. Możliwość monitorowania zajętości CPU.
24. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)

Obsługa Routingu IPv4

25. Sprzętowa obsługa routingu IPv4 – forwarding
26. Pojemność tabeli routingu min. 450 wpisów
27. Routing statyczny
28. Obsługa routingu dynamicznego IPv4 ze wsparciem przynajmniej dla protokołu RI-Pv1/v2.
29. Policy Based Routing dla IPv4
30. Obsługa DHCP/BootP Relay dla IPv4
31. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF.

Obsługa Routingu IPv6

32. Sprzętowa obsługa routingu IPv6 – forwarding
33. Pojemność tabeli routingu min. 225 wpisów
34. Routing statyczny
35. Obsługa routingu dynamicznego dla IPv6 ze wsparciem przynajmniej dla protokołu RIPng.
36. Policy Based Routing dla IPv6.
37. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF v3.

Obsługa Multicastów

38. Statyczne przyłączenie do grupy multicast
39. Filtrowanie IGMP
40. Obsługa Multicast VLAN Registration - MVR
41. Obsługa IGMP v1/v2/v3
42. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo sieciowe

43. Obsługa uwierzytelniania stacji roboczych z wykorzystaniem mechanizmów:
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login

44. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants)
45. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
46. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC
47. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
48. Urządzenie musi wspierać profile bezpieczeństwa, profil bezpieczeństwa oznacza połączenie:
    a. definicji sieci VLAN,
    b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
    c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
    d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
49. Obsługa Guest VLAN dla IEEE 802.1x
50. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
51. Wbudowana obrona procesora urządzenia przed atakami DoS
52. Obsługa TACACS+ (RFC 1492)
53. Obsługa RADIUS Authentication (RFC 2865)
54. Obsługa RADIUS Accounting (RFC 2866)
55. RADIUS and TACACS+ per-command Authentication
56. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
57. Możliwość wyłączenia MAC learning
58. Obsługa SNMPv1/v2/v3
59. Klient SSH2
60. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
61. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
62. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
63. Obsługa bezpiecznego transferu plików SCP/SFTP
64. Obsługa DHCP Option 82
65. Obsługa Gratuitous ARP Protection
66. Obsługa Trusted DHCP Server
67. Obsługa DHCP Snooping
68. Obsługa DHCP Secured ARP/ARP Validation
69. Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x

70. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s
71. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
72. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
73. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
74. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
75. Obsługa PVST+
76. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
77. Obsługa G.8032
78. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
79. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

80. Obsługa synchronizacji czasu NTP lub SNTP
81. Zarządzanie przez SNMP v1/v2/v3
82. Zarządzanie przez przeglądarkę WWW – protokół http i https
83. Telnet Serwer/Klient dla IPv4 / IPv6
84. SSH2 Serwer/Klient dla IPv4 / IPv6
85. Ping dla IPv4 / IPv6
86. Traceroute dla IPv4 / IPv6
87. Obsługa SYSLOG z możliwością definiowania wielu serwerów
88. Sprzętowa obsługa NetFlow lub sFlow
89. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
90. Obsługa RMON2 (RFC 2021)

Inne

91. Obsługa skryptów CLI
92. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
93. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym

Gwarancja

94. Wraz z urządzeniem wymagane jest dostarczenie kontraktu serwisowego na okres min. 1 roku umożliwiającego:

a. bezpłatne aktualizacje oprogramowania firmware,

b. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego od zgłoszenia awarii,

c. wsparcia technicznego producenta poprzez infolinię, pocztę e-mail oraz telefon.

Wyposażenie dodatkowe

95. Wraz z każdym przełącznikiem należy dostarczyć:
    a. niezbędne okablowanie zasilające 230VAC,

5.3.3 Przełącznik LAN

Wymagania podstawowe

1. Przełącznik posiadający min. 48 interfejsów 10/100/1000BASE-T RJ45, min. 4 interfejsy 1GBASE-X SFP oraz 2 interfejsy 10GBASE-X SFP+ do łączenia urządzeń w stos.
2. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
3. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T.
4. Wysokość urządzenia 1U.
5. Przełącznik musi posiadać wbudowany zasilacz 230V AC.
6. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
7. Przełącznik musi posiadać nieblokującą architekturę o wydajności przełączania min. 176 Gbps oraz szybkości przełączania min. 130 Mpps.
8. Musi posiadać możliwość realizacji stosów – łączenia fizycznych przełączników w zarządzane z pojedynczego adresu IP jedno logiczne urządzenie. Do łączenia przełączników muszą być wykorzystane dedykowane interfejsy – bez ograniczania liczby interfejsów uplink. Architektura stosu musi umożliwiać realizację zamkniętej pętli. Wydajność przełączania w stosie min. 40Gbps. Wymagana jest możliwość łączenia do 8 przełączników w stos (w tym również przełączników wspierających technologię PoE).
9. Tablica MAC adresów min. 16k.
10. Pamięć operacyjna: min. 1GB pamięci DRAM.
11. Pamięć flash: min. 2GB pamięci Flash.
12. Pojemność bufora pakietów min. 1,5 MB.
13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
14. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
15. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów).
16. Obsługa Q-in-Q IEEE 802.1ad.
17. Obsługa Quality of Service:
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
18. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
19. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) .
20. Wbudowany DHCP serwer i klient.
21. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
22. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci.
23. Możliwość monitorowania zajętości CPU.
24. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)

Obsługa Routingu IPv4

25. Sprzętowa obsługa routingu IPv4 – forwarding

26. Pojemność tabeli routingu min. 450 wpisów
27. Routing statyczny
28. Obsługa routingu dynamicznego IPv4 ze wsparciem przynajmniej dla protokołu RIPv1/v2.
29. Policy Based Routing dla IPv4
30. Obsługa DHCP/BootP Relay dla IPv4
31. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF.

Obsługa Routingu IPv6

32. Sprzętowa obsługa routingu IPv6 – forwarding
33. Pojemność tabeli routingu min. 225 wpisów
34. Routing statyczny
35. Obsługa routingu dynamicznego dla IPv6 ze wsparciem przynajmniej dla protokołu RIPng.
36. Policy Based Routing dla IPv6.
37. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF v3.

Obsługa Multicastów

38. Statyczne przyłączenie do grupy multicast
39. Filtrowanie IGMP
40. Obsługa Multicast VLAN Registration - MVR
41. Obsługa IGMP v1/v2/v3
42. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo sieciowe

43. Obsługa uwierzytelniania stacji roboczych z wykorzystaniem mechanizmów:
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
44. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants)
45. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
46. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC
47. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
48. Urządzenie musi wspierać profile bezpieczeństwa, profil bezpieczeństwa oznacza połączenie:
    a. definicji sieci VLAN,
    b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
    c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
    d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
49. Obsługa Guest VLAN dla IEEE 802.1x
50. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
51. Wbudowana obrona procesora urządzenia przed atakami DoS
52. Obsługa TACACS+ (RFC 1492)
53. Obsługa RADIUS Authentication (RFC 2865)
54. Obsługa RADIUS Accounting (RFC 2866)
55. RADIUS and TACACS+ per-command Authentication

56. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
57. Możliwość wyłączenia MAC learning
58. Obsługa SNMPv1/v2/v3
59. Klient SSH2
60. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
61. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
62. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
63. Obsługa bezpiecznego transferu plików SCP/SFTP
64. Obsługa DHCP Option 82
65. Obsługa Gratuitous ARP Protection
66. Obsługa Trusted DHCP Server
67. Obsługa DHCP Snooping
68. Obsługa DHCP Secured ARP/ARP Validation
69. Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x
70. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s
71. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
72. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
73. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
74. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
75. Obsługa PVST+
76. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
77. Obsługa G.8032
78. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
79. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

80. Obsługa synchronizacji czasu NTP lub SNTP
81. Zarządzanie przez SNMP v1/v2/v3
82. Zarządzanie przez przeglądarkę WWW – protokół http i https
83. Telnet Serwer/Klient dla IPv4 / IPv6
84. SSH2 Serwer/Klient dla IPv4 / IPv6
85. Ping dla IPv4 / IPv6
86. Traceroute dla IPv4 / IPv6
87. Obsługa SYSLOG z możliwością definiowania wielu serwerów
88. Sprzętowa obsługa NetFlow lub sFlow
89. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
90. Obsługa RMON2 (RFC 2021)

Inne

91. Obsługa skryptów CLI
92. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
93. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym

Gwarancja

94. Wraz z urządzeniem wymagane jest dostarczenie kontraktu serwisowego na okres min. 1 roku umożliwiającego:
    a. bezpłatne aktualizacje oprogramowania firmware,
    b. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego od zgłoszenia awarii,
    c. wsparcia technicznego producenta poprzez infolinię, pocztę e-mail oraz telefon.

Wyposażenie dodatkowe

95. Wraz z każdym przełącznikiem należy dostarczyć:
    a. niezbędne okablowanie zasilające 230VAC,
    b. 1 x kabel do łączenia w stos zapewniający transmisję na poziomie 40Gbps (full duplex) o długości 1m lub zgodnie z projektem wykonawczym

5.3.4 Przełącznik WiFi

Wymagania podstawowe

1. Przełącznik posiadający min. 48 interfejsów 10/100/1000BASE-T RJ45, min. 4 interfejsy 1GBASE-X SFP oraz 2 interfejsy 10GBASE-X SFP+ do łączenia urządzeń w stos.
2. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management.
3. Przełącznik musi wspierać technologię Power over Ethernet (PoE) zgodnie ze standardami IEEE 802.3af (PoE) oraz IEEE 802.3at (PoE+) do zasilania urządzeń takich jak punkty dostępowe WLAN, telefony VoIP i kamery monitoringu wizyjnego.
4. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich interfejsach 10/100/1000BASE-T.
5. Wysokość urządzenia nie więcej niż 1U.
6. Przełącznik musi posiadać wbudowany zasilacz 230V AC zapewniający budżet mocy dla technologii PoE na poziomie min. 740W zapewniając jednocześnie min. 15W dla wszystkich interfejsów 10/100/100BASE-T.
7. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
8. Przełącznik musi posiadać nieblokującą architekturę o wydajności przełączania min. 176 Gbps oraz szybkości przełączania min. 130 Mpps.
9. Musi posiadać możliwość realizacji stosów – łączenia fizycznych przełączników w zarządzane z pojedynczego adresu IP jedno logiczne urządzenie. Do łączenia przełączników muszą być wykorzystane dedykowane interfejsy – bez ograniczania liczby interfejsów uplink. Architektura stosu musi umożliwiać realizację zamkniętej pętli. Wy-

dajność przełączania w stosie min. 40Gbps. Wymagana jest możliwość łączenia do 8 przełączników w stos (w tym również przełączników nie wspierających technologii PoE).

10. Tablica MAC adresów min. 16k.
11. Pamięć operacyjna: min. 1GB pamięci DRAM.
12. Pamięć flash: min. 2GB pamięci Flash.
13. Pojemność bufora pakietów min. 1,5 MB.
14. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
15. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
16. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów).
17. Obsługa Q-in-Q IEEE 802.1ad.
18. Obsługa Quality of Service:
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
19. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
20. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) .
21. Wbudowany DHCP serwer i klient.
22. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
23. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci.
24. Możliwość monitorowania zajętości CPU.
25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)

Obsługa routingu IPv4

26. Sprzętowa obsługa routingu IPv4 – forwarding.
27. Pojemność tabeli routingu min. 450 wpisów.
28. Routing statyczny.
29. Obsługa routingu dynamicznego IPv4 ze wsparciem przynajmniej dla protokołu RI-Pv1/v2.
30. Policy Based Routing dla IPv4.
31. Obsługa DHCP/BootP Relay dla IPv4
32. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF.

Obsługa routingu IPv6

33. Sprzętowa obsługa routingu IPv6 – forwarding.
34. Pojemność tabeli routingu min. 225 wpisów.
35. Routing statyczny.
36. Obsługa routingu dynamicznego dla IPv6 ze wsparciem przynajmniej dla protokołu RIPng.
37. Policy Based Routing dla IPv6.
38. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF v3.

Obsługa ruchu multicast

39. Statyczne przyłączenie do grupy multicast
40. Filtrowanie IGMP
41. Obsługa Multicast VLAN Registration - MVR
42. Obsługa IGMP v1/v2/v3
43. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo sieciowe

44. Obsługa uwierzytelniania stacji roboczych z wykorzystaniem mechanizmów:
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
45. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants)
46. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
47. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC
48. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
49. Urządzenie musi wspierać profile bezpieczeństwa, profil bezpieczeństwa oznacza połączenie:
    a. definicji sieci VLAN,
    b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
    c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
    d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
50. Obsługa Guest VLAN dla IEEE 802.1x
51. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
52. Wbudowana obrona procesora urządzenia przed atakami DoS
53. Obsługa TACACS+ (RFC 1492)
54. Obsługa RADIUS Authentication (RFC 2865)
55. Obsługa RADIUS Accounting (RFC 2866)
56. RADIUS and TACACS+ per-command Authentication
57. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
58. Możliwość wyłączenia MAC learning
59. Obsługa SNMPv1/v2/v3
60. Klient SSH2
61. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection

    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
62. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
63. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
64. Obsługa bezpiecznego transferu plików SCP/SFTP
65. Obsługa DHCP Option 82
66. Obsługa Gratuitous ARP Protection
67. Obsługa Trusted DHCP Server
68. Obsługa DHCP Snooping
69. Obsługa DHCP Secured ARP/ARP Validation
70. Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x
71. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s
72. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
73. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
74. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
75. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
76. Obsługa PVST+
77. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
78. Obsługa G.8032
79. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
80. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

81. Obsługa synchronizacji czasu NTP lub SNTP
82. Zarządzanie przez SNMP v1/v2/v3
83. Zarządzanie przez przeglądarkę WWW – protokół http i https
84. Telnet Serwer/Klient dla IPv4 / IPv6
85. SSH2 Serwer/Klient dla IPv4 / IPv6
86. Ping dla IPv4 / IPv6
87. Traceroute dla IPv4 / IPv6
88. Obsługa SYSLOG z możliwością definiowania wielu serwerów
89. Sprzętowa obsługa NetFlow lub sFlow
90. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
91. Obsługa RMON2 (RFC 2021)
92. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
93. Możliwość uruchamiania skryptów
    a. Ręcznie

b. O określonym czasie lub co wskazany okres czasu
c. Na podstawie wpisów w logu systemowym

Gwarancja

94. Wraz z urządzeniem wymagane jest dostarczenie kontraktu serwisowego na okres min. 1 roku umożliwiającego:
    a. bezpłatne aktualizacje oprogramowania firmware,
    b. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego od zgłoszenia awarii,
    c. wsparcia technicznego producenta poprzez infolinię, pocztę e-mail oraz telefon.

Wyposażenie dodatkowe

95. Wraz z każdym przełącznikiem należy dostarczyć:
    a. niezbędne okablowanie zasilające 230VAC,
    b. 1 x kabel do łączenia w stos zapewniający transmisję na poziomie 40Gbps (full duplex) o długości 1m lub zgodnie z projektem wykonawczym.

6 ZASILANIE AWARYJNE – UPS

Urządzenia aktywne znajdujące się w szafie dystrybucyjnej mają być zabezpieczone poprzez zasilacz awaryjny UPS. Należy zastosować zasilacz awaryjny APC 8000VA wolnostojący, umieszczony poza szafą GPD. Ma on zapewnić prawidłowe działanie urządzeń aktywnych wewnątrz szafy przy maksymalnym poborze mocy 4500 W, na czas około 12min, pozwalając w ten sposób zachować ciągłość pracy tych urządzeń, niezależnie od zakłóceń w dostawach energii elektrycznej z sieci. Należy skonfigurować urządzenia aktywne aby się wyłączyły bezpiecznie.

7 SYSTEM KONTROLI DOSTĘPU (KD)

7.1 Cel systemu kontroli dostępu

Głównym celem systemu kontroli dostępu jest ograniczenie dostępu osobom nie upoważnionym do wyznaczonych stref w budynku biurowym przy ul. Targowej 9 w Gorzowie Wielkopolskim. 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 umożliwia nadzór nad pracownikami, wywołanie alarmu w sytuacji naruszenia chronionego obszaru, zwiększenie bezpieczeństwa zasobów i mienia oraz uniemożliwienie dostępu osobom z zewnątrz.

7.2 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.

7.3 Architektura systemu kontroli dostępu

7.3.1 **Opis ogólny działania systemu**

Za pomocą systemu kontroli dostępu ochroną zostaną objęte wybrane obszary w budynku biurowym przy ul. Targowej 9 w Gorzowie Wielkopolskim, ciągi komunikacyjne, przejścia na klatkę, pomieszczenia oraz inne miejsca wskazane przez Inwestora. Dostęp do stref będzie realizowany przy użyciu kontrolerów drzwiowych oraz czytników kart zbliżeniowych.

Wejście do pomieszczeń/ciągów komunikacyjnych będą realizowane za pomocą karty identyfikacyjnej danej osób mającej dostęp do wyznaczonego pomieszczenia/strefy. Każdorazowe wejście 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 i systemu dozoru wizyjnego (jedna stacja PC). Wszelkie powiadomienia, alarmy oraz raporty będą wyświetlane na zainstalowanym monitorze KD.

7.3.2 **Obszary funkcjonalne**

W budynku zaprojektowano system kontroli dostępu w postaci:

- Kontroli wejścia, składającej się z 10 jednostronnie kontrolowanych drzwi z czujnikiem położenia drzwi, przyciskiem wyjścia po stronie wewnętrznej oraz awaryjnym przyciskiem ewakuacyjnym również po stronie wewnętrznej;

Elementami składowymi systemu kontroli dostępu są:

- Serwer systemu kontroli dostępu z bazą danych;

- Stacja robocza z zainstalowanym oprogramowaniem klienckim (na jednym monitorze KD i CCTV);
- Czytniki kontroli dostępu;
- Kontrolery 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).

7.4 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:

- Zaprojektowano system kontroli dostępu w klasie stopnia ryzyka 2 w skali od 2 do 4 zgodnie z normą PN-EN 60839-11:2014-01;
- 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 ma być obsługiwane przez Główny Punkt Dystrybucyjny GPD znajdujący się na I piętrze w pomieszczeniu serwerowni (1.02);
- Założono zastosowanie kontrolerów działających w sieci Ethernet. Do nich ma zostać doprowadzony kabel ekranowany F/FTP kat.6_A w osłonie zewnętrznej typu LSZH, trudnopalnej i niewydzielającej trujących substancji w obecności ognia (kabel opisany szczegółowo w dokumentacji projektowej okablowania strukturalnego);
- Do wszystkich kontrolerów ma zostać podłączonych w sumie 10 czytników. Kontrola dostępu ma być jednostronna (montaż czytnika kontroli dostępu po stronie zewnętrznej drzwi zgodnie ze schematami ideowymi prowadzenia połączeń dołączonymi do projektu) przy drzwiach;
- System ma posiadać budowę modułową oraz działać online jak i offline (do czasu usunięcia usterki komunikacji z serwem);
- 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 mieć możliwość integracji z systemem SSWiN;
- 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 od 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 musi posiadać rozbudowany moduł służący do zliczania liczby osób w danej strefie kontroli dostępu w celu łatwej i przejrzystej prezentacji listy osób aktualnie znajdujących się w tej strefie oraz posiadać wyraźny wskaźnik prezentujący sumaryczną liczbę osób;
- System ma udostępniać funkcjonalność zarządzania pojazdami;
- System ma udostępniać aplikację Web;
- System ma posiadać funkcję wizualizacji obiektu za pomocą map;
- System ma posiadać funkcję zdalnego otwierania drzwi;
- System ma posiadać możliwość rezerwowania sal;
- 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 ma zapewnić połączenie dedykowanych czytników z kontrolerami za pomocą interfejsu RS-485 lub Wiegand oraz szyfrowania komunikacji za pomocą technologii OSDP v2 (ang. Open Supervised Device Protocol);
- System ma umożliwiać dodanie dodatkowych funkcji wraz ze zmianą potrzeb użytkownika;
- W systemie ma być zagwarantowana możliwość konfiguracji funkcji śluzy dla dowolnej liczby drzwi;
- System musi posiadać wbudowany moduł oprogramowania integrującego SMS (Security Management System).

7.5 Specyfikacja techniczna elementów składowych systemu kontroli dostępu

7.5.1 System kontroli dostępu

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

Oprogramowanie wykorzystuje zaawansowane rozwiązania sprzętowe, obejmujące czytniki kart inteligentnych i kontrolery obsługujące Ethernet, zapewniające również kompatybilność z czytnikami innych producentów. Wykorzystuje 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 następuje z dedykowanej stacji operatorskiej z zainstalowanym oprogramowaniem klienckim.

Oprogramowanie użyte w projekcie jest skutecznym systemem kontroli dostępu i zarządzania SMS (ang. *Security Management System*). Zaprojektowany system kontroli dostępu zapewnia wysoką stabilność i niezawodność. System oferuje pakiet aplikacji klienckich i przeglądarkowych, takich jak monitorowanie alarmów, tworzenie zaawansowanych identyfikatorów, zarządzanie gośćmi, raporty internetowe, integracja

z systemami innych producentów i wiele innych. System działający pod kontrolą systemu Windows oferują przyjazny i łatwy w obsłudze interfejs użytkownika. System obsługuje szereg wiodących w branży produktów sprzętowych wykorzystujących interfejs szeregowy lub sieć Ethernet.

Specyfikacja techniczna

Serwer systemu

W projekcie zastosowano oprogramowanie systemu kontroli dostępu z bazą danych zainstalowane na dedykowanym serwerze (jednostka centralna). Z serwerem kontroli dostępu, poprzez sieć LAN połączone zostaną: 6 kontrolerów, 10 czytników. Oprogramowanie serwera systemu KD zostanie zainstalowane na dedykowanym serwerze umieszczonym w pomieszczeniu serwerowni (1.02) i spełniającym minimalne wymagania sprzętowe przedstawione w tabeli 5.

Tabela 5. Minimalne wymagania dla serwera KD

Nazwa	**Serwer kontroli dostępu**
System operacyjny	Windows 10 (64 bit) lub nowszy
Procesor	Intel Celeron G550
Pamięć RAM	2 GB RAM 1600MHz
Karta graficzna	Zintegrowana
Pamięć minimalna	500GB HDD 7,2k

Stacja operatorska

Zaprojektowano jedną stację operatorską dedykowaną dla obsługi systemu kontroli dostępu KD oraz systemu dozoru wizyjnego CCTV przez operatorów/administratorów/dział kadr. Stacja ma posiadać podzespoły spełniające wymagania systemowe (opisane szczegółowo w dokumentacji systemu dozoru wizyjnego CCTV) do prawidłowego uruchomienia i działania oprogramowania klienckiego oraz możliwości podłączenia monitora KD 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.

W projekcie przewidziano instalację oprogramowania klienckiego na komputerze PC znajdującym się w pomieszczeniu 1.06

Kluczowe funkcje oraz aplikacje dostępne w oprogramowaniu klienckim:

- Identyfikatory VIPPS;
- Zarządzanie pojazdami;
- 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 zagrożeń;
- 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.

7.5.2 **Kontroler drzwi**

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 kontroler obsługujący konfigurację drzwi kontrolowanych jednostronnie. Posiada możliwość połączenia w sieci Ethernet. Posiada wbudowane na płycie łącze Ethernet i komunikuje 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. Kontroler ma być zasilany poprzez zasilacz 12 V DC zainstalowany w obudowie razem z kontrolerem. Kontroler ma mieć podtrzymanie z akumulatora 12 V DC 7 Ah montowanego również w obudowie.

Kluczowe funkcje:

- Kontroler działający w sieci Ethernet w oparciu o protokół internetowy IP;
- Obsługa dwojga drzwi (w trybie jednodrzwiowym oraz dwudrzwiowym);
- Strukturalna baza danych umożliwia przechowywanie do 200 000 użytkowników i do 8 000 operacji w trybie offline;

Specyfikacja techniczna

Kontrolery umieszczone będą w pomieszczeniu serwerowni (1.02) i w pomieszczeniu 0.16 zgodnie z podkładami dołączonymi do projektu. Zasilanie kontrolera będzie zapewnione dzięki zasilaczowi 12 V DC zainstalowanemu w zintegrowanej metalowej obudowie wraz z kontrolerem. Do kontrolera doprowadzony będzie przewód symetryczny skrętkowy 4–parowy o parametrach przewidzianych w dokumentacji projektowej okablowania strukturalnego. Do kontrolera podłączony będzie czujnik położenia drzwi za pomocą przewodu YTDY 2x0,5, przycisk ewakuacji (monitorowanie stanu) YTDY 2x0,5 oraz zamek elektromagnetyczny (przez przycisk ewakuacyjny) za pomocą przewodu OMY 2x1,0.

Tabela 6. Minimalne wymagania dla kontrolera drzwi

Parametry fizyczne	
Wymiary płyty PCB kontrolera	192x145 mm
Obudowa	460x250x90 mm
Waga kontrolera (sama płytka PCB)	0,1 kg
Waga z obudową	5,00 kg
Obudowa	Montowana na ścianie, stalowa
Zasilanie	
Napięcie (tylko płyta PCB)	11–15 V DC
Pobór prądu (bez osprzętu drzwiowego)	170 mA
Napięcie (obudowa - całość)	Wejście 100–240 V AC
Baterie	Integralny obwód ładowania dostarczony wraz z

	obudową oraz dodatkowe baterie
Środowiskowe	
Temperatura pracy	-10° to 55°C
Wskaźniki LED	Zasilanie, Link do hosta, Comms Tx / Rx, Status usterki/ sabotażu, blokady i przekaźnika
Funkcjonalność	
Wyjścia	Min. 2 wyjścia, 12 V DC, 1,5 A max. Dwa wyjścia przekaźnikowe 30V@2A
Wejścia	Pozycja drzwi* Status zamka* Przycisk wyjścia* Interlock* Styk sabotażowy Monitorowanie baterii Dedykowane wejście awarii zasilania (Na przykład awaria zasilania na płycie PCB) * 4-stanowe wejścia zabezpieczone przed manipulacją
Czytniki	Max. 2 czytniki Wiegand
Bateria zapasowa RTC	3,0V akumulator litowo-jonowy
Pamięć użytkowników	do 200 000 użytkowników w trybie offline
Pamięć zdarzeń	do 8 000 operacji w trybie offline
Interfejsy komunikacyjne	
Czytniki	RS485 z szyfrowaną komunikacją
Serwer	10/100BaseT TCP/IP kat.5 UTP, RJ45

7.5.3 **Czytnik kart kontroli dostępu**

Zaprojektowano czytnik kart zbliżeniowych pracujący na częstotliwości 13,56 MHz i współpracujący z zastosowanymi w projekcie kontrolerami. Wielowarstwowe mechanizmy bezpieczeństwa zapewniają autentyczność i poufność danych.

Wielokolorowa dioda LED sterowana przez kontroler oraz biper informują o trybie pracy czytnika i stanie dostępu.

Specyfikacja techniczna

Zastosowano 10 czytników kart zbliżeniowych rozmieszczonych zgodnie z lokalizacjami na dołączonych do projektu podkładach. W tabeli 7 przedstawiono minimalne wymagania dla czytnika.

Tabela 7. Specyfikacja techniczna czytnika

Parametry fizyczne	
Wymiary czytnika	4,8x10,3x2,3 cm
Zasięg odczytu	6 cm (dla kart zastosowanych w projekcie)
Zasilanie	
Napięcie (tylko płyta PCB)	5-16 VDC
Pobór prądu (średni/szczytowy)	60 mA (w stanie czuwania), 200 mA (max)
Interfejs – format	Wiegand, RS485 szyfrowany, Clock-and-Data
Obsługiwane technologie kart – częstotliwość 13,56 MHz	Secure Identity Object (SIO) - iCLASS Seos, iCLASS SE/SR, MIFARE desfire EV1 i MIFARE Classic (domyślnie włączone) - MIFARE Classic i MIFARE DESFire EV1 niestandardowe modele danych,

	- standardowe aplikacje kontroli dostępu iCLASS (standardowe karty iCLASS), - ISO14443A (MIFARE) CSN, ISO14443B CSN, ISO15693 CSN, - FeliCA CSN, CEPAS CSN lub CAN, - MIFARE DESFire EV2 poprzez kompatybilność wsteczną EV1
Temperatura robocza	-35° do 65°C
Temperatura przechowywania	-55° do 85°C
Wilgotność pracy	5% do 95% wilgotność względna, bez skraplania
Miejsce stosowania	Wewnątrz / zewnątrz (IP65)
Gwarancja	Dożywotnia limitowana

7.5.4 **Karty zbliżeniowe**

Użytkownicy systemu kontroli dostępu mają używać kart zbliżeniowych pracujących w paśmie 13,56 MHz.

Karty wykonane są z wysokiej jakości materiałów (kompozyt z 60% PVC / 40% PET), który pozwala na nadruk wszelkiego rodzaju dodatkowych informacji – zdjęć, numerów, itp. Wysoki poziom bezpieczeństwa jest zagwarantowany dzięki szyfrowanej transmisji, która uniemożliwia klonowanie. Podstawowe informacje:

- Karty z pamięcią 8k bajtów bezpieczny procesor;
- Częstotliwość komunikacji: 13,56 MHz w standardzie ISO/IEC 14443 Typ A;
- Typowy maksymalny zasięg odczytu: 7–10 cm (w zależności od wykorzystanego czytnika);
- Wymiary: 5,40x8,57x0,084 cm;
- Temperatura robocza: od -40^{O}C do +70^{O}C;
- Waga: 5,5 g;
- Tryb zachowania bezpieczeństwa (z szyfrowaniem identyfikatorów urządzeń);
- Bezpieczeństwo komunikacji: EN 14890-1 oraz 7816 przy użyciu AES;
- Wytrzymałość zapisu: min. 500 000 cykli;
- Retencja danych: min. 20 lat;
- Chip stykowy: tak;
- Nadruk: tak (biała karta), użytkowy z bezpośrednim obrazowaniem oraz termo transferowe drukarki, obszary wykluczone z drukowania mogą dotyczyć pewnych stref karty;
- Wycięcia: nie dostępne;
- Gwarancja: dożywotnia.

7.5.5 **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.

W przypadku montażu nowych drzwi montaż elektrozamka dobór odpowiedniej listy zaczepowej oraz zamka zatrzaskowego ustalić z producentem stolarki drzwiowej.

Minimalne parametry techniczne jakie musi spełniać elektrozamek przedstawiono w tabeli 8.

Tabela 8. Minimalne wymagania dla elektrozamka

Napięcie	12 V DC
Prąd	max. 0,5A
Tolerancja napięcia zasilania	11 – 15 V DC
Typ	Rewersyjny
Siła trzymania	Min. 250 kg

Zastosowane w projekcie zasilacze kontrolerów konwertują napięcie sieciowe 230 V na napięcie 12 V DC. Zasilacz znajduje się w zamykanej na klucz, metalowej obudowie razem z kontrolerem, w której pozostawiono wolne miejsce na akumulator awaryjny. Zasilacz zapewnia zasilanie wszystkich urządzeń peryferyjnych podłączonych do kontrolera.

7.6 Montaż instalacji oraz prowadzenie okablowania

Kontrolery należy zamontować w pomieszczeniach zgodnie z rzutami dołączonymi do projektu (sugerowany montaż oraz prowadzenie okablowania zostało pokazane na schematach ideowych połączeń systemu kontroli dostępu KD) po stronie wewnętrznej pomieszczeń dla zwiększenia bezpieczeństwa. Dodatkowo kontrolery należy podłączyć do sieci komputerowej przez port RJ45 znajdujący w kontrolerach w celu administracji. Okablowanie do kontrolera zostanie rozprowadzone w pomieszczeniu kablem ekranowanym F/FTP kat.6_A do punktu logicznego PL opisanego szczegółowo w dokumentacji okablowania strukturalnego.

Do kontrolera należy podłączyć czytniki kart za pomocą kabla miedzianego symetrycznego YTDY 8x0.5 mm lub UTP kat.5. 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. YTDY 4x0,5 mm bezdotykowy przycisk wyjścia. YTDY 2x0,5 mm monitorowanie stanu przycisku ewakuacji. Dodatkowo do kontrolera należy połączyć jako wyjście elektrozamek za pomocą kabla OMY 2x1 mm połączony przez odpowiednie styki awaryjnego przycisku wyjścia tak jak to zostało pokazane na schematach ideowych instalacji systemu kontroli dostępu przy drzwiach.

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

- Połączenie Wiegand (czytnik – kontroler) – 150 m (zalecane nie przekraczać 100 m);
- Połączenie kontaktron – kontroler – 600 m;
- Połączenie zasilanie – kontroler – 8 m;
- Połączenie elektrozamek – kontroler – 20 m.

7.7 Zasilanie instalacji

Zasilanie podstawowe:

- Przewiduje się zastosowanie zasilaczy 12 V DC lub 13,8 V DC zamontowanych w metalowej obudowie wraz z kontrolerem jako opcja zasilania podstawowego;
- Przewiduje się zastosowanie akumulatora kwasowo – ołowiowego 12 V DC, 7 Ah zamontowanego w metalowej obudowie wraz z kontrolerem jako opcja zasilania awaryjnego dla kontrolerów.

7.8 Administracja

Wszystkie kontrolery oraz czytniki muszą być oznaczone numerycznie, w sposób trwały. Te same oznaczenia należy umieścić w sposób trwały na gniazdach telekomunikacyjnych na panelach krosowych znajdujących się w szafie dystrybucyjnej GPD.

Konwencja oznaczeń kontrolerów:

KD/X

gdzie:

KD - kontroler kontroli dostępu do drzwi;
X - numer kontrolera.

Konwencja oznaczeń czytników:

KD/X/Y

gdzie:

KD – czytnik kontroli dostępu;
X – numer kontrolera do którego zostanie podłączony;
Y – numer czytnika.

7.9 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.

7.10 Zawartość dokumentacji powykonawczej

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

- Rzeczywiste trasy prowadzenia kabli;
- Rysunki z oznaczeniami szaf dystrybucyjnych, paneli krosowych i portów;
- Lokalizację rzeczywistego rozmieszczenia kontrolerów oraz czytników wraz z udokumentowaniem adresów MAC oraz adresów IP poszczególnych kontrolerów.

7.11 Uwagi dotyczące prowadzenia okablowania

Trasy prowadzenia okablowania zostały skoordynowane z istniejącymi i wykonywanymi instalacjami w budynku biurowym przy ul. Targowej 9 w Gorzowie Wielkopolskim, 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 meta-

lowe 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.

8 INSTALACJA SYSTEMY PRZYWOŁAWCZEGO

8.1 Zakres projektu

Zakres projektu obejmuje instalację przywoławczą dla budynku biurowego przy ul. Targowej 9 w Gorzowie Wielkopolskim 66-400, zlokalizowanym na działce 596/18, obr. Zamoście. Systemem przywoławczym powinny zostać objęte toalety dla niepełnosprawnych w całym budynku:

W odpowiednich obszarach system ma być w pełni zgodny z wymaganiami opisanymi w normie DIN VDE 0834.

System przywoławczy ma zostać zrealizowany w oparciu o sieć LON oraz działać na zasadzie ‘rozporoszonej inteligencji’, gdzie wszystkie urządzenia elektroniczne tworzą samodzielne ‘węzły’ z własnymi procesorami i oprogramowaniem. Nie może wystąpić ‘jeden punkt awarii’, który mógłby mieć wpływ na cały system, dzięki czemu zapewniona zostanie niezawodność systemu i pewność, że pojedyncze punkty awarii zostaną łatwo zlokalizowane, a awarie usunięte.

Przywołania powinny być sygnalizowane za pomocą lampek nad drzwiami do toalet, oraz za pomocą sygnalizatorów akustycznych instalowanych pod lampkami.

8.2 Funkcjonalność

Zasilacz sytemu przywoławczego ma dostarczać do systemu bezpieczne napięcie typu SELV DC. Podtrzymanie UPS ma zapewnić ciągłe działanie systemu w przypadku awarii zasilania sieciowego przez co najmniej 1 godzinę.

Przed wejściem, nad drzwiami do każdej toalety dla osób niepełnosprawnych musi zostać zainstalowana sygnalizacyjna lampa LED wraz z podłączonym sygnalizatorem akustycznym. Ma to na celu sygnalizację wezwań w sposób optyczny i akustyczny. Dla poprawy bezpieczeństwa w miejscach gdzie toalety są słabo widoczne w głównych ciągach komunikacyjnych powinny zostać zainstalowane dodatkowe lampy LED powielające sygnał optyczny z lamp nad toaletami.

Na ścianie toalety przy wejściu musi zostać zainstalowany panel z przyciskami przywołania i kasowania umożliwiający wezwanie pomocy w razie potrzeby oraz skasowanie alarmu. Oba przyciski muszą posiadać diody potwierdzające wciśnięcie przycisku. Dodatkowo dioda przycisku przywołania powinna być cały czas lekko podświetlona w celu ułatwienia lokalizacji przycisku.

Panele z linką pociągową powinny być instalowane na ścianie toalety, tak aby zwisająca linka pociągowa była dostępna z poziomu toalety oraz podłogi. Linka musi być koloru czerwonego i posiadać dwa trójkątne uchwyty na różnych wysokościach. Linka musi być wykonana w taki sposób, aby zerwać się pod obciążeniem większym niż 3,5 kg. Ma to zapobiec uduszeniu w przypadku zaplątania w linkę. Panel musi posiadać diodę potwierdzająca pociągnięcie linki.

Wszystkie panele mają być typu modułowego, aby ułatwić zmianę wykorzystania w razie potrzeby. Przyciski przywołania mają być odpowiednio oznaczone symbolami w sposób umożliwiający szybkie ustalenie ich funkcji. Przyciski mają być kolorowe w celu ułatwienia

identyfikacji ich funkcji. Przyciski przywołania pomocy mają być czerwone. Przyciski kasowania mają być koloru zielonego.

Obudowy paneli z przyciskami przywołania i kasowania, pociągowych, terminali komunikacyjnych oraz lampek LED muszą być wykonane z materiału zawierającego dodatki zwalczające drobnoustroje. Z podobnego materiału muszą być wykonane linki i uchwyty pociągowe paneli pociągowych.

W sekretariacie na pierwszym piętrze musi znajdować się terminal z wyświetlaczem LCD, na którym wyświetlane będą przywołania z całego systemu wraz z ich dokładną lokalizacją. Wyświetlony na ekranie tekst powinien informować o lokalizacji wezwania – np. „WC 1" lub „WC 2". Wyświetlacze powinny także sygnalizować przywołania w sposób akustyczny za pomocą wbudowanych sygnalizatorów akustycznych.

8.3 System przywoławczy – tryb działania

Pacjent przywołuje personel za pomocą czerwonego przycisku lub pociągowego przycisku przywoławczego. Powoduje to następującą sekwencję zdarzeń:

1) Zapala się dioda potwierdzająca na urządzeniu przywoławczym.
2) Zapala się czerwony i biały segment lampy nad drzwiami do toalety, z której pochodzi wezwanie.
3) Na zespole lamp nad drzwiami rozlega się sygnał dźwiękowy (1 sekunda dźwięku na 3 sekundy ciszy, zgodnie z zaleceniami DIN VDE 0834).
4) Informacja o wezwaniu wraz z jego dokładną lokalizacją wyświetlana jest na terminalu w sekretariacie.

Osoba odpowiadająca na wezwanie po udaniu się do właściwej toalety i udzieleniu pomocy ma wcisnąć zielony przycisk kasowania znajdujący się przy wejściu do toalety, z której wystąpiło przywołanie. Powoduje to następującą sekwencję zdarzeń:

1) Gaśnie czerwony i biały segment lampy nad drzwiami do toalety.
2) Ustaje sygnał dźwiękowy.
3) Informacja o wezwaniu znika z wyświetlacza w sekretariacie.

8.4 Szczegółowy opis techniczny elementów systemu

W tabelach zostały przedstawione informacje o poszczególnych elementach systemu. Elementy muszą posiadać parametry i funkcje opisane w poniższych tabelach.

Tabela 9. Zasilacz z UPS

Zasilacz UPS, 27V / 6A w obudowie instalacyjnej	
Zasilanie	230V (195-264V) AC
Pobór prądu	1.2 A
Częstotliwość	50 ± 3Hz
Napięcie wyjściowe	27V +- 1%
Prąd wyjścia	Max. 6 A
Prąd zwarcia	10.7A ± 5%
Obwód wyjściowy	SELV (klasa ochrony III)
Wskaźnik stanu	diody LED
Sprawność	85 %

Stopień ochrony IP	IP 20
Temperatura pracy	od 0 do 40 ^{o}C
Wilgotność	max. 95%, bez kondensacji
Wymiary (SZ x W x G)	400 x 432 x 185 mm
Waga bez baterii	7 kg
Zgodność z normami	DIN VDE 0834
Standardy bezpieczeństwa	EN 62040-1, EN 62368-1
Standardy EMC	EN 61000-6-1, EN 61000-6-3, EN 62040-2

Tabela 10. Bramka TCP/IP

Bramka TCP/IP	
Sposób montażu	szyna DIN 35 x 7.5 mm
Zakres napięcia wejściowego	20 do 27 V DC/ max. 10A
Pobór prądu	190 mA w stanie spoczynku, 350 mA w stanie pracy
Zgodność z normami	DIN VDE 0834
Temperatura pracy	od 0 do 40 ^{o}C
Wilgotność względna	max. 85%, bez kondensacji
Wymiary (SZ x W x G)	246 x 50 x 128 mm
Waga	0.4 kg
Obudowa	PVC/poliamid

Tabela 11. Sygnalizator akustyczny do lampy LED z elektroniką

Sygnalizator akustyczny do lampy LED z elektroniką	
Pobór prądu	10 mA w stanie spoczynku; 75 mA przy maksymalnej głośności
Głośność	Od 45 do 65 dbA z dystansu 2 metrów, możliwość regulacji głośności z poziomu oprogramowania
Temperatura pracy	od 5 do 40 ^{o}C
Wilgotność względna	max. 85%, bez kondensacji
Wymiary (SZ x W x G)	90 x 13 x 33 mm
Waga	0.019 kg
Materiał obudowy	ABS (antybakteryjny)

Tabela 12. Lampa LED z elektroniką

Lampa LED z elektroniką	
Zakres napięcia wejściowego	20 do 27 V DC/ max. 10A
Pobór prądu	20 mA w stanie spoczynku; dodatkowe 20 mA na każdy panel LED; dodatkowo prąd pobierany przez moduły podłączone do lampy (np. sygnalizator akustyczny)
Zgodność z normami	DIN VDE 0834
Stopień ochrony IP	IP 40

Temperatura pracy	od 5 do 40 ^{o}C
Wilgotność względna	max. 85%, bez kondensacji
Wymiary (SZ x W x G)	90 x 110 x 46 mm
Waga	0.159 kg
Materiał obudowy	PC+ABS (antybakteryjny)

Tabela 13. Lampa LED bez elektroniki

Lampa LED z elektroniką	
Zakres napięcia wejściowego	20 do 27 V DC/ max. 10A
Pobór prądu	20 mA na jeden panel świetlny
Zgodność z normami	DIN VDE 0834
Stopień ochrony IP	IP 40
Temperatura pracy	od 5 do 40 ^{o}C
Wilgotność względna	max. 85%, bez kondensacji
Wymiary (SZ x W x G)	90 x 110 x 46 mm
Waga	0.124 kg
Materiał obudowy	PC+ABS (antybakteryjny)

Tabela 14. Panel przywoławczy z przyciskiem przywołania, obecności/kasowania

Panel przywoławczy z przyciskiem przywołania, kasowania	
Zakres napięcia wejściowego	20 do 27 V DC
Pobór prądu	5 mA w stanie spoczynku, max. 23 mA
Stopień ochrony IP	IP 40
Temperatura pracy	od 5 do 40 ^{o}C
Wilgotność względna	max. 85%, bez kondensacji
Montaż	okrągła puszka montażowa
Wymiary	80 x 80 x 13 mm
Waga	0.05 kg

Tabela 15. Panel z linką pociągową

Panel z linką pociągową	
Zakres napięcia wejściowego	20 do 27 V DC
Pobór prądu	3 mA w stanie spoczynku, max. 13 mA
Stopień ochrony IP	IP 42
Temperatura pracy	od 5 do 40 ^{o}C
Wilgotność	max. 95%, bez kondensacji
Linka pociągowa	3m, 2 uchwyty, materiał antybakteryjny
Zgodność z normami	DIN VDE 0834
Wymiary	80 x 80 x 14 mm
Waga	0.083 kg
Materiał obudowy	ABS (antybakteryjny)

Tabela 16 Terminal z wyświetlaczem LCD

Terminal z wyświetlaczem LCD	
Zakres napięcia wejściowego	20 do 27 V DC
Pobór prądu	20 mA w stanie spoczynku; 100 mA z aktywną obecnością
Wyświetlacz LCD	2 x 16 znaków, alfanumeryczny, wysokość znaków: 8 mm (5 x 7 pikseli), rozmiar wyświetlacza 99 x 24 mm (80 x 14 pikseli), podświetlany
Zgodność z normami	DIN VDE 0834
Stopień ochrony IP	IP 40
Temperatura pracy	od 5 do 40 ^{o}C
Wilgotność względna	max. 85%, bez kondensacji
Wymiary (SZ x W x G)	165 x 95 x 32.5 mm
Waga	0.229 kg
Materiał obudowy	ABS
Kolor	Biały (RAL 9010)
Zgodność z normami	DIN VDE 0834

9 OPIS TECHNICZNY MONITORINGU WIZYJNEGO

9.1 Założenia

Podstawą do opracowania projektu systemu dozoru wizyjnego CCTV IP są założenia bezpieczeństwa poczynione przez projektanta w ustaleniu z Inwestorem. Lista norm wykorzystanych w projekcie:

PN-EN 50132-5-1:2012E - Systemy alarmowe -- Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 5-1: Transmisja wideo – Ogólne wymagania eksploatacyjne

PN-EN 50132-5-2:2012E - Systemy alarmowe -- Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 5-2: Protokoły sieciowe (IP) dotyczące transmisji wideo

PN-EN 50132-5-3:2013-04E - Systemy alarmowe -- Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 5-3: Transmisja video – Analogowa i cyfrowa transmisja video

PN-EN 50132-7:2013-04E - Systemy alarmowe -- Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 7: Wytyczne stosowania

PN-EN 62676-1-1:2014-06 - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 1-1: Wymagania systemowe -- Postanowienia ogólne

PN-EN 62676-1-2:2014-06 - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 1-2: Wymagania systemowe -- Wymagania eksploatacyjne dotyczące transmisji wizji

PN-EN 62676-2-1:2014-06 - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 2-1: Protokoły transmisji wizji -- Wymagania ogólne

PN-EN 62676-2-2:2014-06 - Systemy dozorowe 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 dozorowe CCTV stosowane w zabezpieczeniach -- Część 2-3: Protokoły transmisji wizji -- Zastosowanie międzyoperacyjności IP oparte na usługach Web

PN-EN 62676-4:2015-06 - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 4: Wytyczne stosowania

System Exacq Vision cechuje stabilna architektura systemu, wykorzystanie nowoczesnej technologii informatycznej oraz dynamiczny rozwój produktu. System ExacqVision do najnowszych standardów telewizji dozorowej. Dodatkowo system posiada otwarty interfejs programowania aplikacji pozwalający zintegrować system ExacqVision z innymi systemami.

9.2 Wymagania systemu dozoru wizyjnego

- System dozoru wizyjnego VSS otrzymał stopień zabezpieczeń 1 w skali od 1 do 4 zgodnie z normą PN-EN 62676;
- Liczbę i rozmieszczenie elementów systemu dozoru wizyjnego CCTV IP opracowano na podstawie informacji oraz wymagań podanych przez Użytkownika.
- System dozoru wizyjnego CCTV IP powinien zapewniać pełną międzyoperacyjność w komunikacji między wieloma urządzeniami systemu różnych producentów;
- Umożliwienie podłączenia do systemu różnych kamer pochodzących od wielu producentów, w tym obsługa nielimitowanej liczby różnych kamer obsługiwanej przez dedykowane oprogramowanie;
- System powinien zapewniać zdalny dostęp z dowolnego miejsca oraz urządzenia korzystającego z sieci za pomocą dedykowanych, wieloplatformowych aplikacji na urządzenia mobilne (iOS, Windows, Linux, Kindle Fire);
- System powinien zapewnić możliwość przekazywania głosu za pomocą urządzenia mobilnego i przesyłanie go bezpośrednio do wyjścia audio w kamerze;
- Automatyczne wykrywanie podłączonych urządzeń systemu dozoru wizyjnego CCTV IP;
- System ma mieć możliwość rozbudowy o rejestratory hybrydowe, tzn. podłączenie systemu VSS analogowego wraz z systemem VSS cyfrowym wykorzystującym protokół internetowy (IP) do transmisji obrazu oraz zapewniać ich płynne i szybkie działanie;
- System ma mieć dodatkowo możliwość rozbudowy o integrację systemu dozoru wizyjnego VSS z systemami kontroli dostępu, sygnalizacji włamania i napadu;
- Przeszukiwanie nagranego zdarzenia ma odbywać się na podstawie szczególnych wydarzeń w celu skrócenia czasu analizy;
- System powinien mieć możliwość podłączenia kamer kablem sieciowym w oparciu o protokół komunikacyjny TCP/IP;
- Kamery powinny posiadać różne opcje zasilania: PoE, PoE+, 12VDC;
- Kamery powinny obsługiwać następujące rozdzielczości: CIF, 2CIF, 4CIF, D1, 720p, 1080p;
- Kamery powinny wspierać protokoły: TCP/IP, IPv4, TCP, UDP, HTTP, HTTPS, FTP, DHCP, WS-discovery, UPnP, DNS, mDNS, DDNS, RTP, Unicast, Multicast, NTP, IETF NTP, SMTP, WS-security;
- Kamery powinny komunikować się z rejestratorem za pośrednictwem protokołu HTTPS;
- Kamery powinny być zgodne ze standardem ONVIF;
- Kamery powinny posiadać możliwość zapisu z szybkością 30kl/s;

- Kamery mające pracować w warunkach nocnych powinny posiadać podświetlenie IR, o mocy dopasowanej do wymagań klienta odnośnie nadzoru nocą;
- Kamery powinny posiadać możliwość kompresji za pomocą H.264 oraz MJPEG;
- Kamery powinny umożliwiać opcję wydzielenia strumieni wideo;
- Kamery powinny posiadać interfejs sieciowy 10/100 Base –T Ethernet;
- Kamery powinny posiadać możliwość konfiguracji za pomocą przeglądarki WEB;
- Kamery powinny wspierać przeglądarki Internet Explorer, Mozilla Firefox, Google Chrome, Safari;
- Logowanie do strony konfiguracyjnej powinno być zabezpieczone odpowiednim hasłem, a połączenie internetowe powinno być oparte o protokół HTTPS;
- Kamery powinny posiadać możliwość obsługi kart pamięci;
- Kamery powinny wspierać karty pamięci: SD do 4GB, SDHC do 32GB, SDXC 128GB;
- Kamery mające pracować w trudnych warunkach powinny charakteryzować się klasą ochronności IP66 lub IP67;
- Kamery mające pracować w trudnych warunkach powinny być wandaloodporne w stopniu IK10;
- Kamery wewnętrzne powinny prawidłowo pracować w temperaturze od 0˚C do co najmniej 40˚C;
- Kamery zewnętrzne powinny prawidłowo pracować w temperaturze od co najmniej -30˚C do 50˚C;
- Kamery powinny posiadać funkcje dostosowania kontrastu WDR;
- Kamery powinny posiadać możliwość podłączenia zasilania awaryjnego;
- System powinien być w pełni konfigurowalny aby dostosować go do wymagań każdego użytkownika;
- Do każdego użytkownika systemu powinna być możliwość przypisania hasła dostępu oraz nadanie odpowiednich uprawnień;
- System powinien posiadać opcje powiadomień e-mail;
- Ma mieć możliwość wysłania powiadomienia mailowego o zaprogramowanym alarmie z załączonym materiałem wideo (do 10 MB) z tego zdarzenia;
- System powinien udostępniać listę kamer, która można sortować i filtrować w celach organizacyjnych;
- System powinien pozwalać na dodawanie parametru ukrytych przypisanych do kamery (filtry wyszukiwania kamer) takich jak: lokalizacja, adres, miejscowość, wydział, e-mail, numer kontaktowy;
- System powinien pozwalać na konfigurowanie ustawień i funkcji kamer takich jak: edycja nazwy i opisu, zmiana adresu IP, przydzielenie do wyznaczonego folderu lub partycji;
- System powinien umożliwiać konfiguracje ustawień obrazu kamer w tym: rodzaj kompresji, liczbę klatek/s, rozdzielczość, ustawienie strumieniowania;
- System musi mieć możliwość ustawienia minimalnego lub maksymalnego czasu (dni) pozostawienia nagrania dla pojedynczej kamery;
- System musi mieć możliwość zaprogramowania archiwizacji materiału wideo na zewnętrzne macierze dyskowe według ustawień per kamera z określeniem przedziału czasowego o parametrach cały materiał, wykrycie ruchu lub alarmy;
- System powinien obsługiwać i konfigurować strumienie audio kamer;
- System powinien wspierać i obsługiwać kamery PTZ, regulować ich położenie i sterować soczewkami;

- System powinien pozwalać na tworzenie alarmów i łączenie ich z dowolnymi zdarzeniami w systemie np. wykrycie ruchu, zamalowanie kamery, mało pamięci na dysku, utrata połączenia z kamerą itp.;
- System powinien mieć możliwość tworzenia znaczników przez operatora w celu organizacji zaistniałych incydentów;
- System powinien mieć możliwość blokowania nadpisania lub usunięcia materiału wideo, które zostały przypisane do znacznika;
- System powinien pozwalać na wyświetlanie danych z innych systemów na obrazie z kamery;
- Sugeruje się szybkość zapisu na dysku rejestratora sieciowego 12 kl/s, natomiast kamery mają posiadać możliwość rejestracji obrazu z szybkością do 30 kl/s;
- Pamięć dyskowa powinna zapewnić nagrania obrazu wideo co najmniej do 30 dni wstecz przy założeniu zapisu ciągłego z każdej kamery zarówno w ciągu dnia jak i nocy;
- System musi posiadać możliwość podłączenia kamer z ww. zaawansowanymi funkcjami analizy obrazu wideo oraz posiadać możliwość konfigurowania zdarzeń powodowanych przez alarmy przesyłane z kamer oraz łączenia ich z wyzwalaczami programowymi;
- System powinien umożliwiać tworzenie harmonogramów do zapisu wideo, do aktywowania wykrywania ruchu itp.;
- System musi posiadać wbudowane funkcje pozwalające na śledzenie podejrzanych osób przez Operatora w czasie rzeczywistym;
- Ponadto ma zapewnić:
    - Automatyczne wykrywanie podłączonych urządzeń systemu dozorowego VSS;
    - Grupową konfigurację oraz dodawanie kamer do systemu;
    - Możliwość tworzenia konkretnych zdarzeń w systemie dozorowym VSS oraz łączenia ich z systemem kontroli dostępu (powiązywanie zdarzeń z różnych systemów i konfiguracja alarmów);
- Ma posiadać funkcję wtrącenia ważnego wydarzenia podczas obserwacji obrazu z wielu kamer w momencie pojawienia się nietypowego zachowania;
- Wydarzenia/alarmy/powiadomienia systemu dozorowego VSS jak i kontroli dostępu muszą być widoczne z poziomu jednego oprogramowania;
- System powinien umożliwiać podłączenie do 500 klientów za pomocą dedykowanego oprogramowania.

9.3 Opis urządzeń

W budynku zaprojektowano system nadzoru wizyjnego składającego się z 27 kamer. Rozmieszczenie i dobór kamer zostało zaprojektowane z myślą o maksymalizacji bezpieczeństwa. Kamery zewnętrzne znajdują się przy wszystkich wejściach do budynku. Wewnątrz budynku (ciągi komunikacyjne) oraz w pomieszczeniach recepcji zastosowano kamery z szerokokątnym obiektywem.

Sposób oznaczenia kamer:

- KWx – kamera kopułkowa wewnętrzna
- KZx – kamera tubowa zewnętrzna

Oznaczenie kamer na schematach:

Typ kamery_numer kamery

przykład oznaczenia: KW1 – kamera typu W, numer kamery 1

przykład oznaczenia: KZ5 – kamera typu Z, numer kamery 5

Kamery wewnętrzne na korytarzach na sufitach podwieszanych montować w adapterach.

Kamery zewnętrzne montować na dedykowanych puszkach.

9.4 Specyfikacja techniczna kamer użytych w projekcie

Tabela 17. Minimalne wymagania odnośnie kamer wewnętrznych - Kamera wewnętrzna kopułkowa 3 MP

Nazwa	**KWx – kamera kopułkowa wewnętrzna 3MP**
Informacje ogólne	Matryca: 1/2.8” Rozdzielczość: 2048x1536 Szybkość otwarcia migawki: 1/4-1/10000s Min. Oświetlenie: 0.03Lux, 0Lux noc (IR włączony) Poziom S/N: > 50 dB
Funkcje kamery	Dzień/Noc: Mechaniczny ICR WDR: Tak Balans bieli: Auto/Mechaniczny Prywatne strefy: Do 9 stref
Soczewka	Ogniskowa: 2.8-12 mm zmienna Maksymalna apertura: F1.4-2.7 Focus: auto Kąt widzenia: 98°
Obraz	Rodzaj kompresji: H.264/H.265/IntelliZip/MJPEG Dostępne rozdzielczości: 3MP/1080p/720p/D1/CIF Maksymalna liczba klatek na sekundę: Główny strumień: 3MP (30ips) Podstrumień: D1/CIF (30ips)
Parametry sieciowe	Ethernet: RJ-45 (10/100Base-T) Wspierane protokoły: IPv4/IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, ICMP, IGMP, RTSP, RTP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter, QoS, Bonjour Zgodność ze standardem ONVIF: ONVIF Profile S
Pozostałe	Zasilanie: DC12V, PoE (802.3af) Pobór mocy: Max 6W Poziom ochrony IP: IP67, IK10 Temperatura operacyjna: -20°C do 50°C (4°F do 122°F) Wymiary: 123mm x 107mm Waga: 0.97kg

Tabela 18. Minimalne wymagania odnośnie kamer zewnętrznej - Kamera zewnętrzna tubowa 3 MP

Nazwa	**KZx – kamera tubowa zewnętrzna 3MP**
Informacje ogólne	Matryca: 1/2.8” Rozdzielczość: 2048x1536 Szybkość otwarcia migawki: 1/4-1/10000s Min. Oświetlenie: 0.03Lux dzień, 0Lux noc (IR włączony) Poziom S/N: > 50 dB
Funkcje kamery	Oświetlacz podczerwieni: 25m Dzień/Noc: Mechaniczny ICR WDR: Tak Balans bieli: Auto/Mechaniczny Prywatne strefy: Do 9 stref
Soczewka	Ogniskowa: 2.8-12 mm zmienna Maksymalna apertura: F1.4-2.7 Focus: auto Kąt widzenia: 98°
Obraz	Rodzaj kompresji: H.264/H.265/IntelliZip/MJPEG Dostępne rozdzielczości: 3MP/1080p/720p/D1/CIF Maksymalna liczba klatek na sekundę: Główny strumień: 3MP (30ips) Podstrumień: D1/CIF (30ips)
Parametry sieciowe	Ethernet: RJ-45 (10/100Base-T) Wspierane protokoły: IPv4/IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, ICMP, IGMP, RTSP, RTP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter, QoS, Bonjour Zgodność ze standardem ONVIF: ONVIF Profile S
Pozostałe	Zasilanie: DC24V, PoE (802.3af) Pobór mocy: Max 15W Temperatura operacyjna: -40°C do 50°C (-40°F do 122°F) Poziom ochrony IP: IP68, IK10 Wymiary: 70mm x 66mm x 155mm (2.76in x 2.60in x 6.10in) Waga: 1.2kg (2.65lbs)

9.5 Oprogramowanie

System monitorowania oparty jest o oprogramowanie do zarządzania wideo pozwalajace budować systemy wideo IP Wszystkie kamery podłączone do systemu mogą być przeglądane, zarządzane oraz konfigurowane w czasie rzeczywistym. Oprogramowanie zapewnia współ-pracę z wieloma kamerami IP, serwerami oraz systemami pamięci

Ważne funkcje oprogramowania:

Systemowe

- Darmowy klient Win, Linux, Mac
- Podgląd na żywo/zapisanego obrazu przez przeglądarki IE, Chrome, Safari, Opera, Firefox

- Darmowa aplikacja na tablety oraz smartfony, podgląd obrazu na żywo/zapisanego dla Android, iOS, Win8
- Automatyczne znajdowanie, przypisywanie oraz adresowanie kamer IP
- Auto detekcja i możliwość połączenia ponad 2500 kamer od 60 producentów
- Wsparcie dla soczewek fisheye oraz panoramicznych
- Obsługa wydarzeń – eventów
- Możliwość wyzwalania zdarzeń w innych systemach
- Ustawianie różnych czasów przechowywania video dla różnych kamer
- Nagrania TimeLapse
- Podgląd wszystkich modyfikacji systemowych, kto co i jak zmodyfikował
- Tworzenie gryp użytkowników i nadawanie uprawnień
- Integracja z systemem kontroli dostępu, analityki, systemów włamaniowych
- Wyszukiwanie po ruchu w wybranym obszarze video
- Powiadomienia email odnośnie działania systemu

Live View

- Podgląd kamer na wielu monitorach
- Obsługa PTZ oraz definiowanie przejść PTZ
- Cyfrowy PTZ
- Oznaczenia wykrywania ruchu i alarmy
- Automatyczne wykonywanie akcji po wykryciu zdarzenia
- Zdarzenia wyzwalane video, portami szeregowymi oraz pracą systemu
- Przełączanie video za pomocą zdarzeń lub harmonogramu
- Definiowanie grup kamer
- Konfigurowalne zakładki pojawiające się po najechaniu w widoku live
- Nagrywanie wielostrumieniowe
- Powiadomienia email informujące o zdarzeniach
- Dwu kierunkowa komunikacja audio
- Przekazanie widoku dla innych użytkowników

Wyszukiwanie, odtwarzanie, export, archiwizacja

- Bezpośredni replay z widoku live
- Przeszukiwanie video po linii czasu lub za pomocą dzielenia video
- Jednoczesny replay z wielu kamer
- Nagrywanie bezpośrednio na DVD
- Export do .AVI lub plików obsługiwanych przez wbudowany odtwarzacz
- Export widoku z wielu kamer – tylko na wbudowany odtwarzacz
- Trwały zapis, etykietowanie oraz zarządzanie ważnymi plikami video

Pozostałe

- 3 Lata SSA (Subskrypcji aktualizacyjnej)
- Polska wersja językowa

10 INSTALACJA ZASILANIA GWARANTOWANEGO 230V

Dla zasilania sieci komputerowej (bez drukarek), systemu CCTV, systemu KD, systemu przywoławczego systemu sygnalizacji włamania i napadu projektuje się wydzieloną instalację elektryczną 230V współpracującą z UPS.

Główna Rozdzielnica TI+TLK wykonana zostanie i zasilona z rozdzielnicy głównej TGL obiektu.

Dla rozprowadzenia instalacji do wszystkich pomieszczeń na każdej kondygnacji zaprojektowano tablice TBK

Zasilanie instalacji urządzeń komputerowych zaprojektowanych z uwzględnieniem istniejącego sposobu rozdziału energii elektrycznej w obiekcie.

W pomieszczeniach zaprojektowano jedno gniazdo elektryczne potrójne na jedno stanowisko komputerowe oraz maksymalny pobór mocy z jednego zestawu gniazd elektrycznych 300W Przewidziano wydzielone obwody dla szaf krosowniczych z urządzeniami aktywnymi i serwera zasilanych przez UPS;

10.1.1 **Rozdzielnice TBK**

Jako rozdzielnice piętrowe projektuje się skrzynki rozdzielcze z zamkiem. Skrzynki należy wyposażyć w listwę zaciskową N+PE, rozłącznik główny, wyłączniki instalacyjne nadprądowe , wyłącznik różnicowo-prądowy 25A/0,03A, oraz ochronniki przepięciowe zainstalowane dla każdej fazy i przewodu neutralnego. Aparaty te są przeznaczone do montażu na szynie nośnej TH 35 Połączenia wewnętrzne w rozdzielnicach wykonać przy pomocy szyn izolowanych B13 oraz mostków przewodowych.

10.1.2 **Wewnętrzne linie zasilające (WLZ)**

Zasilanie rozdzielnic TBK wykonać zalicznikowym YDYżo 3/5x4 mm2 z rozdzielnicy głównej TI+TLK w korytkach kablowych – (odcinki poziome) – nad sufitem podwieszanym oraz w rurach elektroinstalacyjnych (odcinki pionowe, przejścia przez stropy). Klasa reakcji na ogień przewodów - Dca

10.1.3 **Instalacja gniazd wtyczkowych**

Instalację gniazd wtyczkowych projektuje się przewodem typu YDYpżo 3x2,5 mm2 - 750V układanym pod tynkiem Klasa reakcji na ogień przewodów - Dca

Osprzęt montować w puszkach podtynkowych. Gniazda wtyczkowe należy oznakować w sposób ułatwiający ich identyfikację.

Zastosować gniazda z kluczem tzn. takie, które uniemożliwiają zastosowanie innych urządzeń jak komputerowe.

10.1.4 **5.4. Ochrona przeciwporażeniowa**

Jako środek dodatkowej ochrony od porażeń zastosowano – SAMOCZYNNE WYŁĄCZANIE ZASILANIA w UKŁADZIE TNS. Instalację zasilającą urządzenia komputerowe należy wykonać w układzie sieciowym TN-S.

Przewód ochronny w instalacji należy uziemić podłączając do szyny wyrównawczej GSU.

Rozdzielnice należy oznaczyć i opisać , gniazda elektryczne oznaczyć w ten sposób aby użytkownik mógł identyfikować gniazdo elektryczne z rozdzielnicą piętrową i numerem obwodu , do którego zostało ono podłączone.

Po wykonaniu całej instalacji należy wykonać pomiary odbiorcze.

10.1.5 Ochrona przepięciowa

Spełnienie wymogów ochrony przepięciowej zawartych w normach zrealizować za pomocą ochronników.

10.1.6 Zasilacz awaryjny UPS

Dla wydzielonych obwodów teleinformatycznych budynku zaprojektowano UPS - 8 kVA – 10 minut. UPS i główną rozdzielnicę TI+TLK zabudować w pomieszczeniu technicznym Serwerowni. Pomieszczenie wymaga klimatyzacji i wentylacji.

UPS wyposażyc w:

- ✓ wyłącznik awaryjny p. poż.
- ✓ bypass automatyczny i ręczny (serwisowy)
- ✓ filtr RFI zapewniający spełnienie normy EN 55011/22 poziom B
- ✓ system automatycznej diagnostyki uszkodzeń
- ✓ system łagodnego startu
- ✓ ciekłokrystaliczny panel informujący o stanach zasilacza

Parametry wyjściowe:

- ✓ moc wyjściowa 8kVA
- ✓ napięcie wyjściowe: 220/400 V
- ✓ częstotliwość: 50 Hz +/-1%
- ✓ THDU < 3% dla obciążeń nieliniowych
- ✓ sprawność 91%
- ✓ Baterie bezobsługowe, hermetyczne

10.1.7 5.7. Połączenia wyrównawcze

Dla ograniczenia do wartości niebezpiecznych napięć jakie mogą wystąpić, w pomieszczeniach technicznych wykonać miejscowe połączenia wyrównawcze.

10.2 6. Uwagi końcowe.

Całość wykonać zgodnie z obowiązującymi normami oraz obowiązującymi przepisami. Po wykonaniu instalacji wykonać pomiary skuteczności środków ochrony przeciwporażeniowej oraz rezystancji uziemienia.