



STRONA TYTUŁOWA - PROJEKT BUDOWLANY

egz. nr: ...

DANE OBIEKTU PROJEKTOWANEGO

NAZWA: ROZBUDOWA Z PRZEBUDOWĄ BUDYNKU STAROSTWA POWIATOWEGO PRZY UL. TRAUGUTTA 23 W NIDZICY, STANOWIĄCA ODRĘBNĄ CZĘŚĆ BUDYNKU WRAZ Z ŁĄCZNIKIEM.
PRZEBUDOWA W ZAKRESIE PRAC BUDOWLANYCH W POMIESZCZENIACH PRZYŁĘGŁYCH Z ŁĄCZNIKIEM.
BUDOWA BUDYNKU GARAŻOWO-GOSPODARCZEGO.
ROZBIÓRKA ISTNIEJĄCYCH DWÓCH BUDYNKÓW GARAŻOWYCH.
ZAGOSPODAROWANIE TERENU DZIAŁKI INWESTYCJI Z INFRASTRUKTURĄ TECHNICZNĄ.

NR EWID. DZ.: DZIAŁKA NR: 8/4; 8/5
OBREB: 0005 NIDZICA

JEDN. EWID.: 281104_4 NIDZICA

KATEGORIA OBIEKTÓW BUDOWLANYCH: XVI, VIII

INWESTOR: POWIAT NIDZICKI
UL. TRAUGUTTA 23
13-100 NIDZICA

JEDNOSTKA PROJEKTOWA: G&G PROJEKT
UL. DEKABRYSTÓW 29/2
42-218 CZĘSTOCHOWA
nr. tel.: 889 056 827; 792 696 034

ZAWARTOŚĆ PROJEKTU BUDOWLANEGO:

Zawartość:	TOM 1 Inwentaryzacja, ekspertyza techniczna, projekt rozbiórki TOM 2 Projekt zagospodarowania terenu TOM 3 Projekt branży architektonicznej TOM 4 Projekt branży konstrukcyjnej TOM 5 Projekt branży sanitarnej TOM 6 Projekt branży elektrycznej + branży telekomunikacyjnej TOM 7 Projekt branży drogowej
-------------------	---

TOM 6 – PROJEKT BRANŻY TELEKOMUNIKACYJNEJ

AUTORZY PROJEKTU BUDOWLANEGO:

IMIE I NAZWISKO	UPRAWNIENIA	PIECZĘĆ I PODPIS
Projektant: mgr inż. Joanna Strzelecka	0864/97/U upr. bud. do projektowania w spec. inst. w telekomunikacji przewodowej	
Sprawdzający: inż. Wojciech Gręda	1786/99/U upr. bud. do projektowania i kierowania robotami w spec. inst. w telekomunikacji przewodowej	

SPIS ZAWARTOŚCI OPRACOWANIA

<u>OŚWIADCZENIA, UPRAWNIENIA PROJEKTANTÓW</u>	5-9
1.1 Temat opracowania.....	10
1.2 Zawartość opracowania	10
1.3 Instalacje odbiorcze teletechniczne	10
2.1 Normy i rozporządzenia	11
2.2 Zakres pras	13
2.3 Referencje i dane produktów	13
2.4 Wymogi CPR.....	14
2.5 Odbiór i pomiary	15
2.6 Gwarancja producenta systemu	16
2.7 Dokumentacja powykonawcza.....	17
2.8 Identyfikacja i etykietowanie	17
2.9 Etykietowanie kabli	17
2.10 Etykietowanie paneli	18
2.11 Etykietowanie gniazd	19
2.12 Etykietowanie kabli krosowych	20
2.13 Etykietowanie szaf	20
2.14 Etykietowanie urządzeń sieciowych	20
2.15 Obowiązki Instalatora.....	21
2.16 Wymagania ogólne dotyczące systemu okablowania strukturalnego	21
2.17 Wymagania ogólne dotyczące ochrony i zabezpieczeń infrastruktury IT.....	23
2.18 Prowadzenie okablowania	24
2.19 Separacja okablowania	25
2.20 Piony kablowe	25
2.21 Okablowanie miedziane – punkt logiczny PL.....	25
2.22 System miedziany S/FTP kat. 7 – wymagania	26
2.23 Wymagania dla ekranowanych modułów Rj45 gniazd Kat 6a.....	27
2.24 Wymagania dla ekranowanych wtyków Rj45 kat 6A (MPTL)	29
2.25 Wymagania dla ekranowanych paneli krosowych w wersji prostej	29
2.26 Wymagania dla ekranowanych kabli krosowych miedzianych – wariant 28AWG	30
2.27 Kable światłowodowe wewnętrzne wielomodowe OM4	31
2.28 Minimalne wymagania dla kabli OM4.....	31
2.29 Osprzęt światłowodowy	32
2.30 Punkty dystrybucji okablowania strukturalnego	36
2.31 Wymagania dla szaf stojących w serwerowni o konstrukcji uniwersalnej.....	36
2.32 Wymagania dla Rack 4-słupowy – pomieszczenia PPD	37
2.33 Listwy zasilające PDU i monitoring środowiskowy	38
2.34 Monitoring środowiska.....	41

2.35	Organizacja kabli w szafie.....	42
2.36	Trasy kablowe dla połączeń miedzianych i światłowodowych w Serwerowni.....	43
2.37	Minimalne wymagania dla systemu siatkowych koryt metalowych.....	44
2.38	Obciążenie koryt kablowych	45
2.39	Uziemienie systemu koryt	45
2.40	System zarządzania listwami zasilającymi PDU oraz monitoringiem środowiskowym.....	45
2.41	Minimalne oczekiwana funkcjonalność oprogramowania	46
2.42	Urządzenia sieciowe LAN.....	47
2.43	Wymagania i założenia podstawowe dla poszczególnych części sieci LAN i WLAN ...	48
2.44	Wymagania szczegółowe dla systemów zarządzania i monitorowania infrastrukturą sieciową i dostępem do sieci LAN i WLAN	48
2.45	Wymagania szczegółowe dla systemu zarządzania siecią LAN i WLAN	50
2.46	Wymagania szczegółowe dla kompleksowego systemu kontroli dostępu do sieci.....	53
2.47	Minimalne wymagania techniczne dla wewnętrznego punktu dostępowego sieci bezprzewodowej.	56
2.48	Minimalne wymagania techniczne dla przełącznika rdzeniowego sieci LAN.....	58
2.49	Minimalne wymagania techniczne dla przełączników dostępowych sieci LAN.	60
2.50	Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 48 portowy POE+ 63	
2.51	Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 24 portowy POE+ 63	
2.52	Wsparcie serwisowe	64
2.53	System telefonii VoIP	64
3.1	GENERALNE WYMAGANIA	64
3.2	SYSTEM VMS.....	64
3.3	APLIKACJA KLIENCKA	68
3.4	Ustawianie parametrów pracy kamer [Dla kamer stacjonarnych 1,2,3,5,8 16 i 30 megapikseli].....	70
3.5	Wymagania aplikacji serwerowej i klienckiej w zakresie współpracy i obsługi analizy wideo:	72
3.6	Wymagania dotyczące analizy wideo:.....	72
3.7	Wymagania w zakresie administracji systemem	73
3.8	Mapy w systemie	73
3.9	Sterowanie kamerami PTZ.....	74
3.10	Eksport materiału wideo.....	74
3.11	Wyszukiwanie zdarzeń	75
3.12	Minimalne parametry serwerów dla rejestracji materiału z kamer	76
3.13	KAMERA 12Mpx typu fisheye.....	76
3.14	KAMERA ZEWNĘTRZNA 16MP	77
3.15	OBIEKTYW do kamer 16MP	78
3.16	KAMERA DOME 6MPX	78

3.17	Stacja robocza z monitorami	79
3.18	NASYCENIE PIXELI.....	79
4.1	Terminal łazienkowy	80
4.2	Terminal pokojowy.....	80
4.3	Czytnik resetowania alarmu	80
5.1	Klawiatura dotykowa sensoryczna z wyświetlaczem LCD.....	81
5.2	Zintegrowany Kontroler Systemowy	81
5.3	Moduł rozszerzenia 16 wejść	82
5.4	Zasilacz systemowy 4A.....	82
5.5	Obudowa na szynę DIN	83
5.6	Sygnalizator wewnętrzny akustyczny	83
5.7	Sygnalizator zewnętrzny akustyczno/optyczny.....	83
5.8	Czujka pasywnej podczerwieni	84
5.9	Czujka dualna z antymaskingiem.....	85
6.1	KONTROLER GŁÓWNY	89
8.1	Spis oznaczeń	90
8.2	Sala konferencyjna 2.15	91
8.3	Wytyczne dla branżystów	92
8.4	Wykaz urządzeń.....	92
8.5	Specyfikacja techniczna urządzeń.....	93
8.6	Wykaz linii.....	96
9.1	Opis systemu	98
9.2	Organizacja systemu.....	98
9.3	Elementy systemu.....	99
9.4	Wyświetlacze stanowiskowe	100
9.5	Wyświetlacze główne – monitory.....	100
9.6	Głośniki	100
9.7	Interfejs SAT.....	100
9.8	Interfejs głosowy	101
9.9	Wzmacniacz audio.....	101
9.10	Komputer sterujący	102
 ➤ <u>CZEŚĆ GRAFICZNA:BRANŻA ELEKTRYCZNA</u>		
RZUT PARTERU– INSTALACJE ELEKTRYCZNE		En-1..
RZUT 1 PIĘTRA – INSTALACJE ELEKTRYCZNE		En-2
RZUT 2 PIĘTRA – INSTALACJE ELEKTRYCZNE		En-3



OŚWIADCZENIE PROJEKTANTÓW

Zgodnie z art. 20 ust. 4 Ustawy z dnia 7 lipca 1994r. Prawo budowlane niniejszym oświadczamy, że

PROJEKT BUDOWLANY - TOM 6 Projekt branży telekomunikacyjnej, pn.:

„ROZBUDOWA Z PRZEBUDOWĄ BUDYNKU STAROSTWA POWIATOWEGO PRZY UL. TRAUGUTTA 23 W NIDZICY, STANOWIĄCA ODREBNĄ CZĘŚĆ BUDYNKU WRAZ Z ŁĄCZNIKIEM. PRZEBUDOWA W ZAKRESIE PRAC BUDOWLANYCH W POMIESZCZENIACH PRZYLEGŁYCH Z ŁĄCZNIKIEM. BUDOWA BUDYNKU GARAŻOWO-GOSPODARCZEGO. ZAGOSPODAROWANIE TERENU DZIAŁKI INWESTYCJI Z INFRASTRUKTURĄ TECHNICZNĄ.”

zlokalizowany na działkach nr ewid.: 8/4; 8/5, obręb: 0005 Nidzica został wykonany zgodnie z obowiązującymi przepisami oraz zasadami wiedzy technicznej oraz jest kompletny z punktu widzenia celu jakiemu ma służyć.

BRANŻA TELEKOMUNIKACJI

IMIE I NAZWISKO	UPRAWNIENIA	PIECZĘĆ I PODPIS
Projektant: mgr inż. Joanna Strzelecka	0864/97/U upr. bud. do projektowania w spec. inst. w telekomunikacji przewodowej	
Sprawdzający: inż. Wojciech Gręda	1786/99/U upr. bud. do projektowania i kierowania robotami w spec. inst. w telekomunikacji przewodowej	

Warszawa, dnia 14.11.1997 r.

**Państwowa Inspekcja
Telekomunikacyjna i Poczтовая
Główny Inspektor**

L.dz.GI/DBL/ 4949/97

DECYZJA Nr 0864/97/U

Pani **mgr inż. Joanna Strzelecka**
urodzona dnia **12.04.1954 r. w Łodzi**

Ną podstawie art.104 ustawy z dnia 14 czerwca 1960r.- kodeks postępowania administracyjnego (jednolity tekst - Dz.U. z 1980r. Nr 9, poz. 26 i Nr 27, poz. 111 z późniejszymi zmianami) w związku z § 11 rozporządzenia Ministra Łączności z dnia 10 października 1995r., w sprawie samodzielnych funkcji technicznych w budownictwie telekomunikacyjnym po rozpatrzeniu wniosku, z dnia 10.09.1997 r., w sprawie nadania uprawnień budowlanych w telekomunikacji oraz przeprowadzeniu postępowania kwalifikacyjnego i egzaminu

**nadaje Pani
uprawnienia budowlane w telekomunikacji**

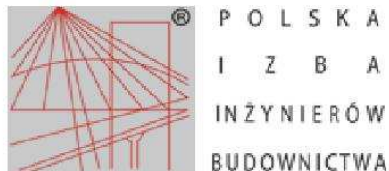
do **projektowania**
w specjalnościach instalacyjnych
w telekomunikacji przewodowej wraz z infrastrukturą towarzyszącą
w zakresie **linii, instalacji i urządzeń liniowych**

Pouczenie

Od niniejszej decyzji służy stronie odwołanie do Ministra Łączności za pośrednictwem Głównego Inspektora PITiP, w terminie 14 dni od dnia jej doręczenia (art. 127 § 1 i 2 oraz 129 § 1 i 2 K.p.).

GŁÓWNY INSPEKTOR
[Podpis]
dr inż. Władysław Grabowski





Zaświadczenie

o numerze weryfikacyjnym:

ŁOD-D68-WTH-ECT *

Pani Joanna STRZELECKA o numerze ewidencyjnym ŁOD/IE/6349/04
adres zamieszkania ul. Przybyszewskiego 119/121 m. 43, 93-110 Łódź
jest członkiem Łódzkiej Okręgowej Izby Inżynierów Budownictwa i posiada wymagane
ubezpieczenie od odpowiedzialności cywilnej.
Niniejsze zaświadczenie jest ważne od 2020-07-01 do 2021-06-30.

Zaświadczenie zostało wygenerowane elektronicznie i opatrzone bezpiecznym podpisem elektronicznym
weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu w dniu 2020-06-29 roku przez:

Barbara Malec, Przewodniczący Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa.

(Zgodnie art. 5 ust 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. 2001 Nr 130 poz. 1450) dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi.)

* Weryfikację poprawności danych w niniejszym zaświadczeniu można sprawdzić za pomocą numeru weryfikacyjnego zaświadczenia na stronie Polskiej Izby Inżynierów Budownictwa www.piib.org.pl lub kontaktując się z biurem właściwej Okręgowej Izby Inżynierów Budownictwa.

Warszawa, dnia 16.11.1999 r.

**Państwowa Inspekcja
Telekomunikacyjna i Poczta
Główny Inspektor**

L.dz.GI/DBL/ 4701 /99

DECYZJA Nr 1786/99/U

Pan inż. Wojciech Gręda
urodzony dnia 07.05.1971 r. w Warszawie

Na podstawie art.104 ustawy z dnia 14 czerwca 1960r.- kodeks postępowania administracyjnego (jednolity tekst - Dz.U. z 1980r. Nr 9, poz. 26 i Nr 27, poz. 111 z późniejszymi zmianami) w związku z § 11 rozporządzenia Ministra Łączności z dnia 10 października 1995r., w sprawie samodzielnych funkcji technicznych w budownictwie telekomunikacyjnym po rozpatrzeniu wniosku, z dnia **23.08.1999 r.**, w sprawie nadania uprawnień budowlanych w telekomunikacji oraz przeprowadzeniu postępowania kwalifikacyjnego i egzaminu

**nadaje Panu
uprawnienia budowlane w telekomunikacji**

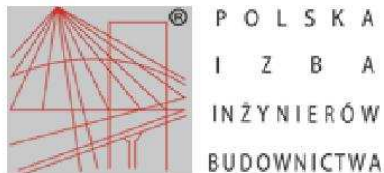
do projektowania i kierowania robotami budowlanymi
 w specjalnościach instalacyjnych
w telekomunikacji przewodowej wraz z infrastrukturą towarzyszącą
w zakresie linii, instalacji i urządzeń liniowych

Pouczenie

Od niniejszej decyzji służy stronie odwołanie do Ministra Łączności za pośrednictwem Głównego Inspektora PITiP, w terminie 14 dni od dnia jej doręczenia (art.127 §1 i 2, art.129 §1 i 2 Kpa)



GŁÓWNY INSPEKTOR
dr inż. Władysław Grabowski



Zaświadczenie

o numerze weryfikacyjnym:

ŁOD-EJV-X7X-F7H *

Pan Wojciech GRĘDA o numerze ewidencyjnym ŁOD/BT/6521/04

adres zamieszkania ul. Lelewela 25 m. 66, 93-166 Łódź

jest członkiem Łódzkiej Okręgowej Izby Inżynierów Budownictwa i posiada wymagane ubezpieczenie od odpowiedzialności cywilnej.

Niniejsze zaświadczenie jest ważne od 2020-10-01 do 2021-09-30.

Zaświadczenie zostało wygenerowane elektronicznie i opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu w dniu 2020-09-07 roku przez:

Barbara Malec, Przewodniczący Rady Łódzkiej Okręgowej Izby Inżynierów Budownictwa.

(Zgodnie art. 5 ust 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. 2001 Nr 130 poz. 1450) dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi.)

* Weryfikację poprawności danych w niniejszym zaświadczeniu można sprawdzić za pomocą numeru weryfikacyjnego zaświadczenia na stronie Polskiej Izby Inżynierów Budownictwa www.piib.org.pl lub kontaktując się z biurem właściwej Okręgowej Izby Inżynierów Budownictwa.

1. OPIS TECHNICZNY

Podstawa opracowania:

- umowa zawarta z Inwestorem,
- projekty branżowe
- warunki techniczne
- opinia geotechniczna
- obowiązujące normy i przepisy
- wizja lokalna

1.1 Temat opracowania

Tematem opracowania są instalacje słaboprądowe w projektowanym Starostwie w Nidzicy

1.2 Zawartość opracowania

Niniejsza dokumentacja zawiera:

- opis techniczny,
- rysunki techniczne.

1.3 Instalacje odbiorcze teletechniczne

W budynku starostwa projektuje się montaż następujących instalacji słaboprądowych:

- Instalacji okablowania strukturalnego/LAN,
- Instalacji SSWIN/KD/Rejestracji czasu pracy,
- instalacji systemu CCTV,
- Instalacji systemu przywołania,
- Instalacji AV,
- Instalacji systemu kolejkowego.

2. INSTALACJA OKABLOWANIA STRUKTURALNEGO/DOSTĘP DO SIECI TELETECHNICZNEJ

Dostęp do sieci teletechnicznej zrealizowany zgodnie z istniejącymi warunkami technicznymi dostępu do sieci teletechnicznej – projektowany GPD należy połączyć za pomocą światłowodu 8J do istniejącego GPD w istniejącej części starostwa. Instalacja okablowania strukturalnego i telefonicznego będzie obejmowała cały budynek.

Przedmiotem niniejszego opracowania jest projekt instalacji systemu okablowania strukturalnego dedykowanego dla wszelkich systemów wykorzystujących sieć Ethernet IP (np. LAN, WLAN, VoIP, HD-Base-T, CCTV, KD, System Przywoławczy, Oświetlenie LED, Digital Signage i inne). Wszelkie rozwiązania budynkowe które wykorzystują system okablowania strukturalnego muszą być bezwzględnie oparte o system spełniający wszystkie poniższe wymagania.

Niniejszy projekt opisuje minimalne wymagania Inwestora w zakresie technicznym i funkcjonalnym. Oznacza to, że należy zastosować rozwiązania spełniające wszystkie kryteria opisane w niniejszej dokumentacji, tj. zgodne pod kątem obowiązującej normalizacji, wymaganych parametrów oraz funkcji.

2.1 Normy i rozporządzenia

Podstawą do opracowania projektu okablowania strukturalnego są wymagania Inwestora w zakresie funkcjonalności i wydajności systemu oraz obowiązujące normy:

- **PN-EN 50173:2018-07** – Technika Informatyczna. Systemy okablowania strukturalnego:
 - **PN-EN 50173-1** – Wymagania ogólne;
 - **PN-EN 50173-2** – Budynki biurowe;
 - **PN-EN 50173-3** – Zabudowania przemysłowe;
 - **PN-EN 50173-4** – Zabudowania mieszkalne;
 - **PN-EN 50173-5** – Centra danych;
 - **PN-EN 50173-6** – Rozproszone usługi budynkowe;
- **PN-EN 50174-1:2018-08** – Technika informatyczna. Instalacja okablowania:
 - **PN-EN 50174-1** – Specyfikacja instalacji i zapewnienie jakości;
 - **PN-EN 50174-2** – Planowanie i wykonawstwo instalacji wewnątrz budynków;
 - **PN-EN 50174-3:2014-02/A1:2017-07** – Planowanie i wykonawstwo instalacji na zewnątrz budynków;
- **PN-EN 50310:2016-09** – Sieć połączeń wyrównawczych w budynkach i innych obiektach budowlanych z instalacjami telekomunikacyjnymi;
- **PN-EN 50346:2004/A1:2009+A2:2010** – Testowanie zainstalowanego okablowania
- **PN-EN 61280-4-1:2010** – Procedury badań światłowodowych podsystemów telekomunikacyjnych – Zainstalowana sieć kablowa – Pomiar tłumienności światłowodów wielomodowych;
- **PN-EN 61280-4-2:2014-11** – Procedury badań światłowodowych podsystemów telekomunikacyjnych – Zainstalowane okablowanie – Pomiary tłumienia i tłumienności odbicia w przypadku światłowodów jednomodowych;
- **IEC 61935-1:2019** – Specification for the testing of balanced and coaxial information technology cabling - Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards;
- **ISO/IEC 14763-2:2019** – Information technology — Implementation and operation of customer premises cabling — Part 2: Planning and installation;
- **ISO/IEC TR 14763-2-1:2011** – Information technology — Implementation and operation of customer premises cabling — Part 2-1: Planning and installation - Identifiers within administration systems;
- **ISO/IEC 14763-3:2014/Amd1:2018** – Implementation and operation of customer premises cabling - Part 3: Testing of optical fibre cabling;

- **ISO/IEC 14763-4:2018** – Information technology — Implementation and operation of customer premises cabling — Part 4: Measurement of end-to-end (E2E)-Links;
- **IEC 61280-4-1:2019** – Fibre-optic communication subsystem test procedures - Part 4-1: Installed cabling plant - Multimode attenuation measurement;
- **IEC 61280-4-2:2014** – Fibre-optic communication subsystem test procedures - Part 4-2: Installed cable plant - Single-mode attenuation and optical return loss measurement;
- **IEC 61300-3-1:2005** – Fibre optic interconnecting devices and passive components - Basic test and measurement procedures - Part 3-1: Examinations and measurements - Visual examination;
- **IEC 61280-4-4:2017** – Fibre optic communication subsystem test procedures - Part 4-4: Cable plants and links - Polarization mode dispersion measurement for installed links;
- **ISO/IEC 30129:2015/Amd:2019** – Amendment 1 - Information technology - Telecommunications bonding networks for buildings and other structures;
- **ANSI/TIA-568.0-E:2020** – Generic Telecommunications Cabling for Customer Premises;
- **ANSI/TIA-568.1-E:2020** – Commercial Building Telecommunications Cabling;
- **ANSI/TIA-568.2-D:2018** – Balanced Twisted-Pair Telecommunications Cabling and Components;
- **ANSI/TIA-568.3-D:2016** – Optical Fiber Cabling and Components Standard;
- **TIA-942-B:2017** – Telecommunications Infrastructure Standard for Data Centers;
- **TIA-569-E:2019** – Telecommunications Pathways and Spaces;
- **ANSI/TIA-1005-A:2012/Reaffirmed:2020** – Telecommunications Infrastructure Standard for Industrial Premises;
- **ANSI/TIA-862-B:2016/AD:2017** – Structured Cabling Infrastructure Standard for Intelligent Building Systems;
- **ANSI/TIA-606-C:2017** – Administration Standard for Telecommunications Infrastructure;
- **ANSI/TIA-607-D:2019** – Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises;
- **ANSI/TIA-1152-A:2016** – Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling;
- **Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 305/2011 w sprawie wyrobów budowlanych (CPR)**
- **Dyrektywa Parlamentu Europejskiego i Rady 2011/65/UE z dnia 8 czerwca 2011r. w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym**

Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami opisanymi w niniejszej dokumentacji oraz powołanymi i powiązanymi z nimi normami a także zastosować się obligatoryjnie do wszelkich wymagań producenta stosowanego systemu okablowania strukturalnego w celu objęcia go po instalacji gwarancją systemową na okres min. 25 lat.

Jeśli którykolwiek z dokumentów normalizacyjnych uległ aktualizacji w stosunku do wymienionych powyżej, należy każdorazowo stosować najnowsze wydania normalizacyjne.

2.2 Zakres prac

Zakres planowanych prac polega na instalacji, testowania oraz wdrożenia kompletnego systemu okablowania strukturalnego. Obejmuje to co najmniej następujące zadania:

- a. Koordynacja prac z głównym wykonawcą oraz dostawcami rozwiązań;
- b. Zarządzanie projektem;
- c. Zarządzanie planowaniem;
- d. Szczegółowa analiza funkcjonalna systemu do zatwierdzenia przez Klienta;
- e. Szczegółowa dokumentacja systemu do zatwierdzenia przez Klienta;
- f. Transport, rozładunek i składowanie na miejscu sprzętu;
- g. Instalacja sprzętu;
- h. Konfiguracja sprzętu;
- i. Integracja systemu okablowania strukturalnego z systemami budynkowymi;
- j. Kompletnie testowanie zainstalowanego systemu (testy jednostkowe, testy integracyjne, testy odbiorcze, testy użytkowników itp.);
- k. Szkolenie Klienta z zakresu poprawnej eksploatacji i obsługi;
- l. Zapewnienie bezproblemowej możliwości rozbudowy systemu w przyszłości;
- m. Dostarczenia narzędzi niezbędnych do konserwacji systemu;
- n. Dostarczenie dokumentacji powykonawczej (podręczniki dla użytkowników, instrukcje konserwacji, raporty z pomiarów itp.);
- o. Wykonawca systemu okablowania strukturalnego (SOS) musi ściśle współpracować z dostawcą urządzeń aktywnych do sieci LAN w celu zapewnienia matrycy połączeń fizycznych od portu przełącznika sieciowego aż do urządzenia końcowego;
- p. Wykonawca systemu okablowania strukturalnego (SOS) musi ściśle współpracować z dostawcą urządzeń aktywnych do sieci LAN w celu dostarczenia odpowiednich elementów (dukty) wspomagających dostarczanie zimnego powietrza do przełączników w przypadku stosowania rozwiązań aktywnych z przepływem powietrza z boku na bok szafy;

Powyższa specyfikacja określa dostawę, instalację, certyfikację, testowanie i udzielenie gwarancji na kompletny system okablowania pochodzący od jednego producenta.

Wykonawcy projektowanego systemu powinni dokładnie ocenić dołączone do projektów Przedmiary, specyfikacje i wszelkie powiązane rysunki dla realizowanych systemów.

2.3 Referencje i dane produktów

— Wykonawca musi przedstawić w swojej ofercie: szczegółowe karty katalogowe producenta oferowanych produktów w tym dane dotyczące funkcjonalności, spełnianych standardów oraz wydajności a dodatkowo:

- a. Imię i Nazwisko inżyniera odpowiedzialnego za realizację projektu;
- b. Szczegóły gwarancji proponowanych przez wykonawcę i producenta;
- c. Kopia gwarancji producenta określająca obowiązki, środki zaradcze, ograniczenia i wykluczenia;
- d. Świadectwa szkoleń przedstawicieli Wykonawcy z zakresu instalacji proponowanego systemu SOS;
- e. Lista pracowników technicznych Wykonawcy biorących udział w instalacji systemu SOS wraz z potwierdzeniem ich kompetencji i doświadczenia;

- f. Lista narzędzi używanych do instalacji oraz testowania systemu SOS;
- g. Dokumentacja techniczna wraz z numerami katalogowymi proponowanych komponentów;
- h. Katalog urządzeń;

Dla każdego rodzaju oferowanego produktu należy podać charakterystykę działania, specyfikację i akcesoria. Każdy produkt należy odnieść do lokalizacji na rysunkach.

Dane dotyczące produktów muszą zawierać co najmniej następujące informacje:

- a. Zestawienie materiałów wraz z numerami katalogowymi;
- b. Nazwa i adres producenta;
- c. Oświadczenie o zgodności ze specyfikacją wraz z niezbędnymi dokumentami uzupełniającymi;
- d. Karty katalogowe proponowanego sprzętu;
- e. Nazwa i adres autoryzowanego lokalnego przedstawiciela / dystrybutora;

Wykonawca dostarczy podpisane przez producentów komponentów zaświadczenie, że dostarczone produkty są zgodne z wymogami.

Dodatkowo należy dostarczyć certyfikaty zgodności normatywnej wydawane przez niezależne laboratoria badawcze (np.: Intertek, GHMT, Delta) dla komponentów wchodzących w skład toru transmisyjnego (kable, złącza, kable krosowe)

2.4 Wymogi CPR

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

Proponowany dostawca okablowania powinien klasyfikować swoje obecne europejskie portfolio kabli miedzianych i światłowodowych poziomych, wykorzystując zatwierdzone jednostki notyfikowane i tym samym zapewniając zgodność z wymaganiami Rozporządzenia o Wyrobach Budowlanych (CPR).

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

W przypadku produktów wymienionych w tym dokumencie CPR dotyczy kabli miedzianych i światłowodowych. CPR określa, jak kable reagują w warunkach pożaru (tj. właściwości spalania, takie jak przenoszenie ognia, wytwarzanie dymu, kwas i płonące krople itp.).

Poziom wydajności kabli jest oznaczony przez tzw. Euroklasy. Euroklasy są hierarchiczne, co oznacza, że można stosować materiały o wyższym oznaczeniu we wszystkich parametrach. Różne kraje mają różne minimalne wymagania Euroklas.

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

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

2.5 Odbiór i pomiary

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

- wykonanie instalacji w sposób estetyczny, zgodny ze sztuką i obowiązującymi normami,
- wykonanie kompletu pomiarów,
- opracowanie i przekazanie dokumentacji powykonawczej Inwestorowi,
- uzyskanie gwarancji systemowej producenta okablowania.

Wykonawstwo pomiarów sieci miedzianej Klasy E_A powinno być zgodne z normą IEC 61935-1. Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą ISO/IEC 14763-3. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

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

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

a) Pomiary okablowania miedzianego

- Analizator okablowania wykorzystany do pomiarów sieci miedzianej musi charakteryzować się przynajmniej V klasą dokładności dla Klasy E_A wg IEC 61935-1 (proponowane urządzenia to np. FLUKE DSX5000 lub DSX8000).
- Pomiary sieci miedzianej dla Klasy E_A należy wykonać na zgodność z ISO/IEC11801 lub EN50173-1 zachowując następującą kolejność:
 1. Łącze stałe (Permanent Link) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego,
 2. Kable krosowe przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego,
 3. Kanał (Channel) przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego,
- Pomiary łączy wykorzystujących wtyki MPTL należy wykonać zgodnie z ANSI-TIA568.2-D dla Klasy E_A wykorzystując odpowiednie adaptery pomiarowe specyfikowane przez producenta sprzętu pomiarowego dla danej klasy okablowania,
- 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.

b) Pomiary światłowodów

Przed dokonaniem jakichkolwiek połączeń pomiarowych do mierzonych torów światłowodowych należy zastosować procedurę inspekcji oraz czyszczenia złącz, adapterów oraz transceiverów światłowodowych zarówno od strony mierzonego toru jak i przyrządów i kabli pomiarowych. Procedura czystości złącz światłowodowych musi być zgodna z normą IEC 61300-3-35 co musi zostać udokumentowane protokołami pomiarowymi.

- Tłumienie światłowodowego toru transmisyjnego ma być wyznaczone za pomocą miernika OLTS a dodatkowo zaleca się wykonanie pomiarów OTDR,
- Przy pomiarze OTDR należy użyć rozbiegówki oraz dobiegówki w celu określenia jakości wszystkich złączy,
- Podczas pomiaru OLTS należy wykorzystać metodę pomiarową z 1 kablem referencyjnym,
- Dla połączeń światłowodowych opartych o kable wielomodowe (jeżeli występują) należy bezwzględnie wykorzystywać kable pomiarowe Encircled Flux;
- Kompletny pomiar każdego duplexowego toru transmisyjnego wykonanego OLTS i OTDR powinien być przeprowadzony w dwie strony w dwóch oknach transmisyjnych dla dwóch włókien:
 - od punktu A do B w oknie 1310nm i 1550nm dla światłowodów jednomodowych
 - od punktu B do A w oknie 1310nm i 1550nm dla światłowodów jednomodowych
 - od punktu A do B w oknie 850nm i 1300nm dla światłowodów wielomodowych
 - od punktu B do A w oknie 850nm i 1300nm dla światłowodów wielomodowych

2.6 Gwarancja producenta systemu

Gwarancja na system okablowania strukturalnego oraz akcesoria ma spełniać poniższe warunki:

- gwarancja ma być jednolitą bezpłatną usługą serwisową świadczoną przez Producenta systemu okablowania (tj. bez ponoszenia jakichkolwiek kosztów przez Użytkownika w przyszłości związanych z przeglądami, serwisowaniem czy innymi pracami związanymi z naprawą i powtórą instalacją wadliwych elementów);
- ma obejmować całość okablowania miedzianego oraz światłowodowego wraz z kablami krosowymi i innymi elementami niezbędnymi do budowy sieci takimi jak panele krosowe, gniazda i wtyki RJ45, adaptery światłowodowe, pigtaile itp.;
- minimalny czas trwania gwarancji systemowej okablowania strukturalnego to 25 lat,
- minimalny czas trwania gwarancji na szafy to min. 12 miesięcy,
- minimalny czas trwania gwarancji na listwy PDU to min. 36 miesięcy,
- gwarancja ma być udzielana na oficjalnych warunkach, ogólnie znanych i opublikowanych;
- gwarancja ma być udzielona przez producenta okablowania bezpośrednio Inwestorowi / Użytkownikowi.

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

2.7 Dokumentacja powykonawcza

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

- Raporty z pomiarów dynamicznych okablowania,
- Rzeczywiste trasy prowadzenia kabli z lokalizacją przebiegów przez ściany, podłogi, itp.
- Rysunki elewacji szaf z oznaczeniami poszczególnych szaf, paneli krosowych i portów,
- Rzuty z naniesionymi gniazdami.

2.8 Identyfikacja i etykietowanie

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

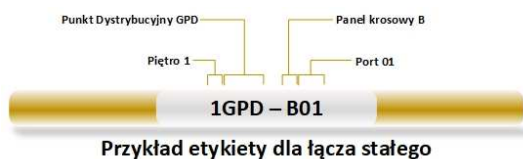
Należy oznaczyć wszelkie:

- Kable,
- Kable krosowe,
- Panele krosowe,
- Szafy i stojaki,
- Gniazda logiczne,
- Urządzenia sieciowe.

2.9 Etykietowanie kabli

Wszystkie kable systemowe muszą zostać oznaczone w sposób trwały umożliwiający jednoznaczne określenie pochodzenia i miejsca przeznaczenia za pomocą niepowtarzalnego identyfikatora.

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, zarówno od strony gniazda PL, jak i od strony szafy montażowej w zależności od przeznaczenia wg. poniższej specyfikacji:



Przykład etykiety dla łącza stałego

1GPD-B01



Przykład etykiety dla połączenia między różnymi Punktami Dystrybucyjnymi

GPD.1-35.08.LNK



Przykład etykiety dla połączenia między szafami w obrębie jednego pomieszczenia

GPD1-35:08/GPD2-12:18

Etykiety muszą być umieszczone 75mm od końca kabla.

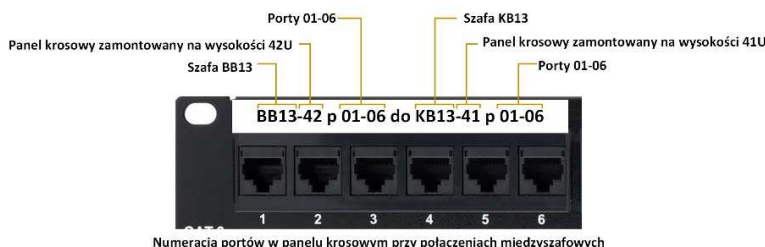
Do etykietowania kabli należy użyć etykiet spełniających poniższe wymagania:

- Wielkość etykiety dobrana odpowiednio do średnicy kabla;
- kolor biały z czarnym nadrukiem termo-transferowym;
- etykieta samo-laminująca;
- etykieta samoprzylepna;
- wytrzymałość temperaturowa w przedziale od -40°C do 66°C;
- odporność UV do min: 3000 godzin;
- zgodność z RoHS;

2.10 Etykietowanie paneli

Panele krosowe należy oznaczać w następujący sposób:

- panele krosowe oznaczają alfabetycznie zaczynając od lewego górnego rogu i dalej w dół;
- numeracja portów w panelu jeżeli nie są one fabrycznie ponumerowane powinna zaczynać się od lewej strony i dalej w prawo;



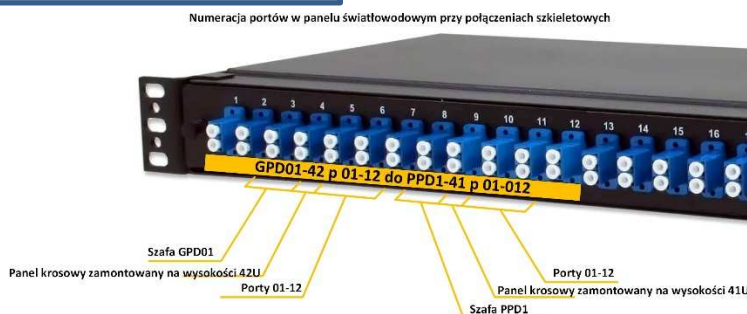
Numeracja portów w panelu krosowym przy połączeniach międzyszafowych



Numeracja portów w panelu krosowym dla okablowania poziomego

BB13-42 p 01-06 do KB13-41 p 01-06

B01, B02 ...



GPD01-42 p 01-12 do PPD1-41 p 01-12

Do etykietowania paneli krosowych należy użyć etykiet spełniających poniższe wymagania:

- Wielkość etykiety dobrana odpowiednio do wielkości pola opisowego;
- kolor biały z czarnym nadrukiem termo-transferowym;
- etykieta winylowa;
- etykieta samoprzylepna;
- wytrzymałość temperaturowa w przedziale od -40°C do 90°C;
- odporność UV do min: 3000 godzin;
- zgodność z RoHS;

2.11 Etykietowanie gniazd

Gniazdach telekomunikacyjnych w obszarach roboczych należy oznaczać w następujący sposób:



1GPD-B01

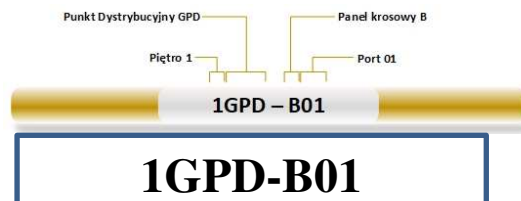
Do etykietowania gniazd należy użyć etykiet spełniających poniższe wymagania:

- Wielkość etykiety dobrana odpowiednio do wielkości pola opisowego;
- kolor biały z czarnym nadrukiem termo-transferowym;
- etykieta winylowa;
- etykieta samoprzylepna;
- wytrzymałość temperaturowa w przedziale od -40°C do 90°C;
- odporność UV do min: 3000 godzin;

— zgodność z RoHS;

2.12 Etykietowanie kabli krosowych

Kable krosowe muszą posiadać oznaczenia umożliwiające jednoznaczne przyporządkowanie końcówki do określonej szafy / panela / portu wg. poniższego schematu



Etykiety muszą być umieszczone 75mm od końca kabla krosowego.

Do etykietowania kabli krosowych miedzianych należy użyć etykiet spełniających poniższe wymagania:

- Wielkość etykiety dobrana odpowiednio do przekroju stosowanego patchcordu;
- kolor biały z czarnym nadrukiem termo-transferowym;
- etykieta samolaminująca;
- etykieta samoprzylepna umożliwiająca po przyklejeniu obrót etykiety w lewo lub w prawo dla wygodnego odczytywania oznaczenia;
- wytrzymałość temperaturowa w przedziale od -40°C do 65°C;
- odporność UV do min: 3000 godzin;
- zgodność z RoHS;

2.13 Etykietowanie szaf

Szafy oraz Racki otwarte powinny odznaczać się unikalną i jednoznaczną numeracją. Numery powinny zostać umieszczone na górze szafy w części środkowej.

Przykład numeru szafy



Do etykietowania szaf i racków należy użyć etykiet spełniających poniższe wymagania:

- Wielkość etykiety powinna zostać dobrana w taki sposób aby oznaczenie było dobrze widoczne z odległości min. 1,5m;
- kolor biały z czarnym nadrukiem termo-transferowym;
- etykieta winylowa;
- etykieta samoprzylepna;
- wytrzymałość temperaturowa w przedziale od -40°C do 90°C;
- odporność UV do min: 3000 godzin;
- zgodność z RoHS;

2.14 Etykietowanie urządzeń sieciowych

Umieść na urządzeniu sieciowym etykietę w dostępnym miejscu z przodu i z tyłu,

zawierającą odpowiedni identyfikator, adres MAC i datę instalacji. Etykieta nie może zakłócać działania urządzenia ani łączyć się z nim ani zasłaniać etykiet producenta.

Do etykietowania gniazd należy użyć etykiet spełniających poniższe wymagania:

- Wielkość etykiety dobrana odpowiednio do wielkości dostępnego obszaru;
- kolor biały z czarnym nadrukiem termo-transferowym;
- etykieta winylowa;
- etykieta samoprzylepna;
- wytrzymałość temperaturowa w przedziale od -40°C do 90°C;
- odporność UV do min: 3000 godzin;
- zgodność z RoHS;

2.15 Obowiązki Instalatora

W celu ujawnienia procedury, jak również zapoznania Użytkownika/Inwestora z prawami, obowiązkami i ograniczeniami gwarancji, wykonawca ma potwierdzić, procedury, warunki i tryb udzielenia gwarancji Użytkownikowi.

W celu weryfikacji aktualnego statusu certyfikowanego instalatora Producent oferowanego systemu musi udostępniać informację o aktualnym stanie aktywnych certyfikowanych instalatorów na swojej stronie internetowej lub pisemnie na życzenie Inwestora.

Wykonawca ma posiadać na dzień składania oferty status aktywnego certyfikowanego instalatora oraz zatrudniać przynajmniej 2-óch pracowników przeszkolonych w zakresie instalacji, pomiarów, nadzoru, wykrywania oraz eliminacji uszkodzeń wg. programu szkoleń Producenta.

Dokumenty mają być przedstawione Zamawiającemu przed podpisaniem umowy.

Dostarczone elementy pasywne wraz z szafami i organizerami kabli 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.

2.16 Wymagania ogólne dotyczące systemu okablowania strukturalnego

- System okablowania strukturalnego należy wykonać w oparciu o elementy jednego producenta.
- Producent okablowania ma posiadać w ofercie oraz dostarczyć; system okablowania miedzianego, światłowodowego, szafy dystrybucyjne wraz z organizerami oraz system dystrybucji energii dla urządzeń aktywnych – listwy PDU wraz z oprogramowaniem do zarządzania listwami PDU oraz sensorami środowiskowymi;
- Listwy PDU muszą umożliwiać podłączenie czujników do monitoringu warunków środowiskowych w pomieszczeniach dedykowanych na punkty dystrybucyjne oraz w Serwerowni;
- Producent oferowanego rozwiązania musi posiadać w swojej ofercie min. następujące sensory oraz inne elementy do podłączenia do listwy PDU:
 - Temperatury;
 - Temperatury + wilgotności;
 - 3x temperatura + wilgotność;
 - Liniowy czujnik zalania;

- Punktowy czujnik zalania;
- Wejście styku bez potencjałowego;
- Kontaktron drzwiowy;
- HUB dostępowy dla kontroli dostępu do szafy (wymagana obsługa technologii kart 125kHz i 13,56MHz);
- Listwa oświetleniowa LED;
- HUB rozszerzenia portów sensorów
- Oprogramowanie musi umożliwiać raportowanie oraz alarmowanie o przekroczeniu zadanych parametrów z sensorów za pomocą maila;
- Oprogramowanie do zarządzania listwami PDU oraz sensorami monitorowania środowiska ma być kompatybilne i w pełni zintegrowane z systemem monitoringu warstwy fizycznej sieci LAN (system miedziany i światłowodowy) oraz systemem zarządzania zasobami IT tak aby Użytkownik w dowolnym momencie mógł rozbudować system o te funkcjonalności;
- Rozmieszczenie stanowisk roboczych przyjęto na podstawie ustaleń z Użytkownikiem oraz najbardziej aktualnej aranżacji wnętrz dla pomieszczeń na etapie projektowania;
- Piętrowe Punkty Dystrybucyjne (PPD_0, PPD_1, PPD_2) należy zlokalizować w Pomieszczeniach PPD;
- Główny Punkt Dystrybucyjny (GPD) należy zlokalizować w pomieszczeniu Serwerowni;
- Serwerownia powinna być zrealizowana zgodnie z najlepszymi praktykami;
- Pomieszczenie Serwerowni musi zawierać:
 - Odpowiednia powierzchnia na umieszczenie ilości szaf wg. potrzeb Klienta,
 - Dostęp do szaf z każdej strony,
 - Możliwość swobodnego otwarcia drzwi w szafach, zarówno z przodu szafy jak i od tyłu,
 - Monitoring środowiska w szafach – min. temperatura, wilgotność, punktowy czujnik zalania,
 - Możliwość zabudowy szaf w kiosk z zamkniętym korytarzem,
 - Wyposażenie w niezbędne systemy bezpieczeństwa takiej jak: monitoring CCTV, Kontrolę dostępu do pomieszczenia KD, Detekcja pożaru, Klimatyzację,
 - Kanały kablowe dedykowane dla połączeń miedzianych i światłowodowych,
- Połączenia szkieletowe wewnątrzbudynkowe należy zrealizować w oparciu o kable światłowodowe wielomodowe z włóknami OM4:
 - 1x12 włókien
- Wszelkie połączenia światłowodowe szkieletowe należy zakończyć na przełącznicach światłowodowych z wykorzystaniem złącz typu:
 - LC
- Na potrzeby komunikacji głosowej wykorzystany zostanie system VoIP który będzie wykorzystywał projektowaną sieć LAN;
- Montaż gniazd okablowania poziomego PL ma być realizowany podtynkowo przy zastosowaniu płyt czołowych z uchwytyami w standardzie montażowym 45x45;
- Okablowanie poziome spełniające wymogi minimum kat.6A ma być prowadzone miedzianym kablem typu:
 - S/FTP kat.7
- Okablowanie miedziane ma być realizowane poprzez moduły gniazd RJ45 o wydajności:

- Ekranowane kat.6A
- Należy zastosować panele krosowe typu:
 - 24 porty, 1U, modułarne:
 - Wersja prosta,
- Wszystkie kable okablowania poziomego mają być zakończone w osprzęcie połączeniowym zgodnie z normą PN-EN 50173-1;
- W celu podniesienia bezpieczeństwa użytkowania okablowania, przy zachowanym standardzie złącza RJ45, należy wykorzystać mechaniczne zabezpieczenia - gniazda dostępne dla osób niepowołanych powinny umożliwiać ich zaślepienie zabezpieczając przed niepowołanym podłączeniem się do sieci. O ich udostępnieniu osobie trzeciej powinien decydować administrator sieci zdejmując za pomocą specjalnego klucza blokadę – zaślepkę gniazda.
- Aby zagwarantować i potwierdzić wymaganą wydajność okablowania miedzianego przeznaczonych do zabudowy (kabel oraz gniazdo) producent musi posiadać certyfikaty wydane przez akredytowane niezależne laboratoria (np. Intertek, ETL, GHMT, Delta) potwierdzające zgodność systemu/komponentów z wymaganiami normy międzynarodowej, tj. ISO/IEC 11801 lub EN50173-1;
- Wszystkie złącza światłowodowe muszą być wypolerowane w fabrycznym procesie produkcyjnym;
- Dla każdego podsystemu (np. LAN, Systemy bezpieczeństwa) należy stosować kable krosowe oraz moduły gniazd RJ45 w odpowiednim kolorze dla łatwej identyfikacji i zarządzania systemem – tym samym nie dopuszcza się stosowania rozwiązań, które wykorzystują oznaczenia kolorystyczne w formie dodatkowych naklejek/ikon itp.;
- Wszystkie miedziane kable krosowe muszą pochodzić od tego samego producenta co reszta komponentów okablowania strukturalnego oraz posiadać deklarację zgodności CE;
- Wszystkie miedziane wtyki kablowe stosowane w połączeniach MPTL muszą pochodzić od tego samego producenta co reszta komponentów okablowania strukturalnego oraz posiadać deklarację zgodności CE;
- W szafach stojących mają być zastosowane wieszaki poziome i pionowe ułatwiające prowadzenie i układanie kabli oraz zarządzanie kablami krosowymi;
- Producent proponowanego systemu okablowania strukturalnego musi posiadać od przynajmniej 7 lat aktualne certyfikaty ISO 9001 i ISO 14001;

2.17 Wymagania ogólne dotyczące ochrony i zabezpieczeń infrastruktury IT

W dobie zagrożeń związanych z cyberatakami infrastruktura IT wymaga ochrony na każdym poziomie dostępu także tym fizycznym. Dla pełnego bezpieczeństwa i kontroli dostępu do sieci musimy mieć możliwość zabezpieczenia wszelkich portów sieciowych jak i USB poprzez które można dostać się do krytycznych zasobów firmy lub instytucji. Instalowane rozwiązania muszą gwarantować Użytkownikowi zapewnienie maksymalnej ochrony sieci na poziomie warstwy fizycznej w następujących aspektach:

- Fizyczna kontrola dostępu do portów sieciowych miedzianych i światłowodowych;
 - Mechaniczne zabezpieczenia uniemożliwiające podłączenie do sieci urządzeń nieautoryzowanych zarówno dla interfejsów miedzianych (RJ45) jak i światłowodowych (LC). Wszelkie porty wymagające tych zabezpieczeń należy

wyposażyc w zaślepki.

- Kolorystyczne kodowanie portów miedzianych oraz kabli krosowych;

Kolorystyczne kodowanie portów miedzianych i kabli krosowych pozwala wyodrębnić część infrastruktury sieciowej dedykowanej grupie lub określone podsystemowi np. (CCTV, KD, WiFi) dzięki czemu uzyskujemy dużą transparentność przy zarządzaniu oraz eliminujemy błędy połączeniowe w infrastrukturze sieciowej;

- Ochrona infrastruktury teleinformatycznej w serwerowni i pomieszczeniach z punktami dystrybucyjnymi na wypadek zalania, wzrostu temperatury oraz wilgotności;

Monitorowanie przy pomocy dedykowanych sensorów zainstalowanych w szafie oraz pomieszczeniu.

- Monitorowanie stanu połączeń warstwy fizycznej AIM;

UWAGA: Wszystkie zabezpieczenia (zaślepki) portów miedzianych RJ45 i USB muszą być obsługiwane za pomocą unikalnego klucza umożliwiającego usunięcie blokad z gniazd. Nie może być możliwości usunięcia blokad w inny sposób.

2.18 Prowadzenie okablowania

Okablowanie w budynku ma zostać rozprowadzone:

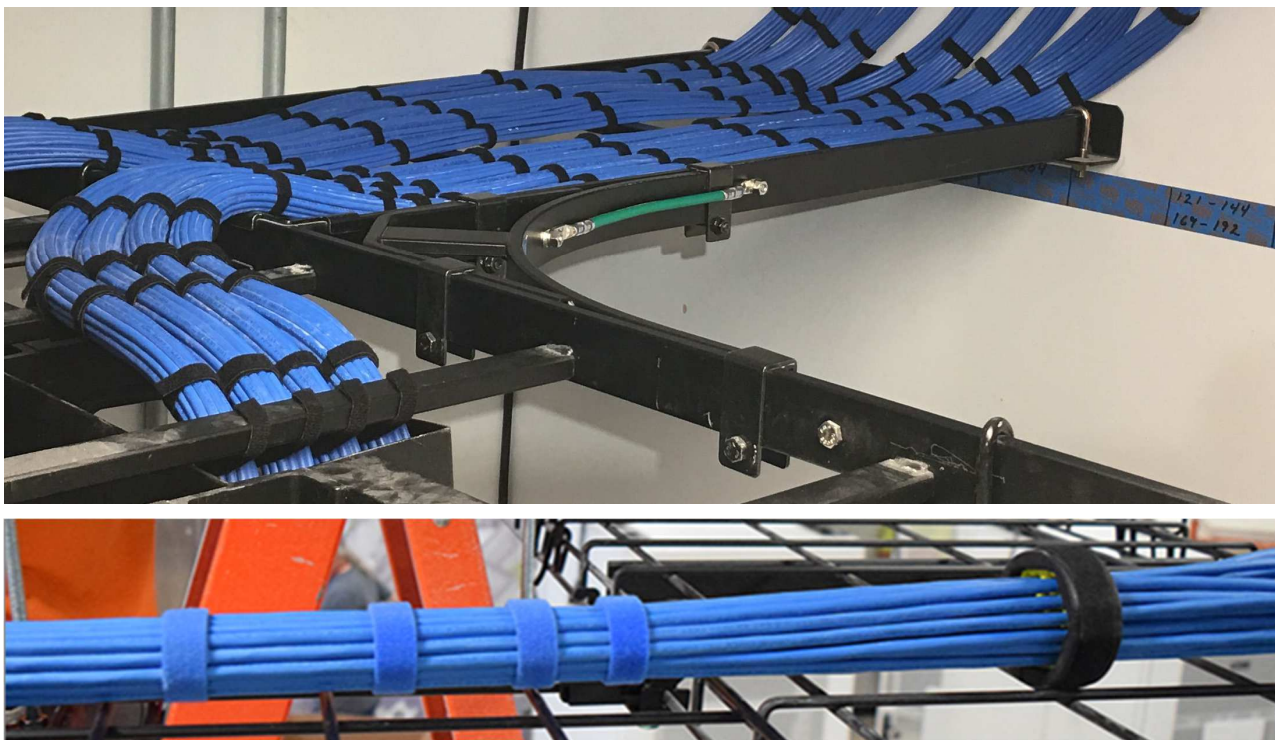
- na głównych ciągach komunikacyjnych w korytach kablowych umieszczonych w przestrzeni między sufitowej lub pod sufitem – należy zabezpieczyć przynajmniej 30% rezerwy na rozbudowę okablowania w przyszłości,
- w pomieszczeniach do punktu logicznego – podtynkowo w rurkach peszel,

Okablowanie w Serwerowni ma zostać doprowadzone do szaf z wykorzystaniem montowanych pod sufitem dedykowanych kanałów kablowych dla systemów miedzianych oraz niezależnych dedykowanych kanałów kablowych dla systemów światłowodowych. Kanały kablowe należy doprowadzić bezpośrednio nad dach szaf dystrybucyjnych dla łatwego wprowadzania przewodów do szafy.

Kable miedziane wchodzące do punktów dystrybucyjnych oraz serwerowni należy organizować w wiązki po max.24 sztuki od punktu wejścia do pomieszczenia aż do panela krosowego w szafie. Przygotowane wiązki przewodów należy przy pomocy specjalnych grzebieni precyzyjnie cesać, spinać tylko opaskami rzepowymi (*nylonowe opaski zaciskowe w przestrzeni punktów dystrybucyjnych oraz serwerowni są zabronione*) i układać pod podłogą techniczną lub w korytach kablowych nad szafami zachowując odpowiednie promienie gięcia oraz najwyższą estetykę wykonania. Opaski rzepowe należy stosować min. co 50cm na odcinkach prostych oraz min. co 25cm na wszelkich łukach i zakrętach.

UWAGA:

Wiązki kablowe które nie będą wykonane w należyty sposób nie zostaną zakwalifikowane jako należyte wykonanie.



2.19 Spręż okablowań

Kable okablowania strukturalnego oraz elektrycznego, należy prowadzić w oddzielnych trasach kablowych przy zachowaniu minimalnej separacji. Wartość separacji kabli logicznych od elektrycznych należy obliczyć zgodnie z normą **PN-EN 50174-2:2018-08**

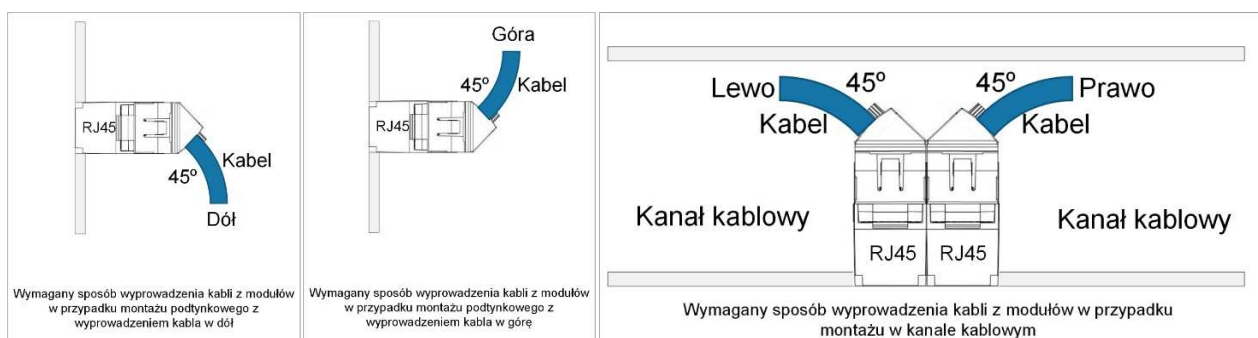
2.20 Piony kablów

Trasy kablów pionowe mają być zbudowane z drabinek kablowych w wydzielonych szachtach dla instalacji teleinformatycznych. Na każdej kondygnacji należy zainstalować drzwiczki rewizyjne przy szachcie kablowym przy podłodze i suficie.

2.21 Okablowanie miedziowe – punkt logiczny PL

Kable okablowania poziomego mają być zakończone w zestawach gniazd, zwanych dalej punktami logicznymi (PL). Gniazda w zestawach PL występują w różnej ilości i konfiguracji w zależności od lokalizacji i przeznaczenia.

Zestawy gniazd PL mają być zgodne ze standardem uchwyty osprzętu elektroinstalacyjnego typu M45 (45x45mm). Należy zastosować płyty czołowe skośne. Rodzaj płyty czołowej należy tak dobrać, aby płyta czołowa nie powodowała nadmiernego promienia gięcia kabla po zatrzaśnięciu w ramce. Należy stosować także odpowiednio głębokie puszki podtynkowe lub kanały kablów, aby pozostawić odpowiedni zapas przestrzeni dla kabla i modułu po zatrzaśnięciu w ramce. Dodatkowo należy stosować moduły gniazd, które pozwalają wyprowadzić kabel pod kątem 45° w górę, dół, lewo lub w prawo w zależności od kierunku, z którego kabel wchodzi do PL – patrz rysunki poniżej. Taki sposób wyprowadzenia kabli z modułów gwarantuje optymalny promień gięcia kabli oraz poprawne parametry kanału nawet w ograniczonych przestrzeniach.



Dla urządzeń IoT, jeżeli jest to technicznie i funkcjonalnie uzasadnione należy stosować wtyki MPTL – wtyki RJ45 montowane bezpośrednio na skręcie. Przykładowe miejsca zastosowania to: WLAN, CCTV, KD itp. Taki sposób realizacji połączenia znacząco upraszcza topologie pod warunkiem spełnienia wymagań opisanych w normie EN 50173-6. Producent oferowanego rozwiązania musi posiadać w swojej ofercie odpowiednie wtyki RJ45 – patrz wymagania szczegółowe dla wtyków RJ45. **Połączenie zrealizowane w topologii MPTL musi zostać poddane pomiarom i certyfikacji w celu uzyskania gwarancji na te łącza.**

Rozmieszczenie stanowisk roboczych przyjąć na podstawie ustaleń z Użytkownikiem oraz najbardziej aktualnej aranżacji wnętrz dla pomieszczeń na etapie realizacji inwestycji; Do PL doprowadzić odpowiednią ilość kabli symetrycznych 4-parowych. Kable należy zakończyć gniazdami RJ45 lub wtykami RJ45 w zależności od przeznaczenia konkretnego kanału transmisyjnego.

W związku z mocnym zróżnicowaniem urządzeń podłączonych do sieci IP należy przyjąć jednoznaczne przyporządkowanie kolorystyczne modułów RJ45 w gniazdach i panelach krosowych. Rozwiązanie takie zapewnia administratorowi sieci łatwą i szybką orientację od strony szafy kablowej a pracownikom użytkującym sieć nie pozwala na pomyłki związane z wpinaniem się do sieci w nieodpowiedni port. Przyjęta kolorystyka ma mieć odzwierciedlenie w rysunkach szaf kablowych.

Kolor modułu RJ45	Przeznaczenie
Czerwony	LAN dla systemów bezpieczeństwa
Niebieski	LAN ogólnego przeznaczenia
Zielony	LAN dla Wydział Komunikacji
Wtyk MPTL	Systemy bezpieczeństwa / strona urządzenia

2.22 System miedziany S/FTP kat. 7 – wymagania

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 7,2mm (co determinuje maksymalną średnicę żyły na 23 AWG). Nie dopuszcza się kabli o większej średnicy zewnętrznej. Instalacja ma być poprowadzona podwójnie ekranowanym kablem konstrukcji S/FTP z osłoną zewnętrzną trudnopalną (LSZH).

W związku z potrzebą zapewnienia jak najlepszych parametrów dla szybkich aplikacji 1G/10G i uzyskania najwyższej odporności przed zakłóceniami należy zastosować kable ekranowane kategorii 7 o konstrukcji S/FTP (każda para ekranowana za pomocą folii aluminiowej oraz wspólny ekran dla wszystkich par z oplotu z siatki stalowej). Podwójny ekran doskonale redukuje zakłócenia zarówno niskich jak i wysokich częstotliwości w tym

ANEXT zapewniając doskonałe parametry transmisyjne dla wszystkich częstotliwości do 650MHz.

Minimalne wymagania dla kabli miedzianego S/FTP kategorii 7;

- Średnica zewnętrzna kabla – max. 7.2mm;
- Przekrój żyły przewodnika – 23AWG;
- Rodzaj osłony zewnętrznej: LSFRZH;
- Euroklasa – Dca-s1a,d1,a1;
- Gwarancja pełnego wsparcia PoE i zgodności z wymaganiami IEEE 802.3af i IEEE 802.3at, IEEE 802.3bt dla aplikacji PoE;
- Temperatura pracy: -20°C do +60°C;
- Zgodność z ISO 11801, ANSI/TIA-568-C.2, IEEE 802.3an, IEC 61156-5, IEC 60754-2, IEC 61034, IEC 60332-1-24;
- Certyfikat zgodności normatywnej niezależnego laboratorium dla min. 4 połączeń w kanale dla ISO 11801 Klasa EA;

Testy mechaniczne	
Minimalny promień gięcia	8 x średnica kabla
Testy elektryczne	
NVP	76%

2.23 Wymagania dla ekranowanych modułów RJ45 gniazd Kat 6a

W opisane płyty czołowe należy zamontować ekranowane dwuelementowe moduły gniazda RJ45 kat. 6A. Moduł gniazda RJ45 ma posiadać konstrukcję dwuelementową, składającą się z części przedniej (z interfejsem RJ45 oraz złączami IDC dla par transmisyjnych) oraz części tylnej. Metalowa obudowa (zarówno na części przedniej i tylnej) podczas montażu gniazda ma się składać w szczelną całość. Konstrukcja modułu nie może zniekształcać konstrukcji kabla, ma również zapewniać maksymalną łatwość instalacji oraz gwarantować najwyższe parametry transmisyjne. Wymaga się, aby każdy moduł gniazda RJ45 posiadał możliwość uniwersalnego terminowania kabli, tj. w sekwencji T568 A lub B. Każdy moduł ma być zarabiany narzędziami. Wymagane jest, wykorzystanie do montażu takich narzędzi, które terminują gniazdo (wszystkie 8 żył) poprzez jeden ruch narzędzia, zapewniając krótkie rozploty par max. 6mm (a przez to najlepsze możliwe osiągi transmisyjne) oraz dużą powtarzalność i szybkość zarabiania – **tym samym nie dopuszcza się modułów gniazd, które terminowane są metodą narzędzia uderzeniowego lub bez narzędzi.**

Dla zapewnienia w kanale transmisyjnym odpowiednich parametrów dla przesyłu szybkich aplikacji takich jak 1G/10G oraz pełne wsparcie dla najnowszych wymagań PoE należy zastosować moduły ekranowane RJ45 kategorii 6A wysokiej klasy.

Minimalne wymagania dla ekranowanych modułów gniazd RJ45:

- Zgodność z ISO 11801 Kategoria 6A/Klasa EA, ANSI/TIA-568.2-D, IEEE 802.3an;
- Wymagany certyfikat na kanał transmisyjny w konfiguracji 4-złączowej do 100m;
- Wymagany certyfikat komponentowy dla modułu RJ45 kat.6A;
- Gwarancja pełnego wsparcia PoE i zgodności z wymaganiami IEEE 802.3af i IEEE 802.3at, IEEE 802.3bt (typ 3 i 4) dla aplikacji PoE, PoE+, PoE++ dla minimum 2500 cykli połączeniowych;
- Wsparcie dla PoH (Power over HDBaseT do 100W);

- Gniazda muszą być zgodne z wymaganiami metod badawczych określonych w normach IEC 60512-9-3 i IEC 60512-99-001 w celu zapewnienia, że w przypadku wystąpienia łuku elektrycznego nie uszkodzi to krytycznego punktu styku wtyku i gniazda.
- Temperatura pracy: -10°C do +65°C;
- Zgodność z ANSI/TIA-1096A; IEC 60603-7, RoHS
- Styki gniazda muszą być pokryte min. 50 µcal złota dla najwyższej wydajności;
- Zapewnia ekranowanie 360° zintegrowane z modułem – bez dodatkowych elementów ekranujących dokładanych do gniazda;
- Zapewnia stabilne połączenie elektryczne z panelem krosowym w celu prawidłowego uziemienia;
- Producent oferowanych modułów ma mieć dostępne w ofercie moduły przynajmniej w 6-ciu kolorach do wyboru (preferowane kolory: czarny, niebieski, zielony, czerwony, żółty, fioletowy);
- Od strony paneli krosowych należy stosować moduły z automatyczną sprężynową zintegrowaną kłapką przeciw kurzową zapewniającą ochronę min. IP40;
- Każdy moduł ma być przetestowany w 100% przez producenta w celu zapewnienia wydajności NEXT i RL a następnie indywidualnie oznakowany numerem seryjnym;
- Konstrukcja modułów musi umożliwiać upakowanie do 48 portów w panelu 1U;
- Moduł podczas terminowania ma zapewniać optymalną wydajność poprzez zachowanie geometrii par i zminimalizowanie rozplotu;
- Terminowanie modułu ma zapewniać poprawne umieszczenie przewodników w nożach wykorzystując płynny ruch bez konieczności uderzania w wewnętrzne komponenty modułu;
- Możliwość terminowania 4 par w tym samym momencie;
- Konstrukcja modułu musi umożliwiać wyprowadzenie kabla pod kątem 45° z tyłu modułu w zależności od potrzeby w lewo, prawo, do góry i w dół;
- Dopuszczalna grubość akceptowanego przewodnika to 22-26AWG w wykonaniu drut i linka;
- Moduł musi być oznaczony kolorami w celu łatwego rozpoznania schematu rozszycia T568A i T568B;

Wymagane parametry mechaniczne

Rodzaj testu	Metoda badania	Pomiar	Wynik testów
Siła normalna	-	Obciążenie (gramy)	>100
Trwałość	IEC 512-9a	Rezystancja obwodu (mΩ)	<40
Podłączanie / Odłączanie	IEC 512-3b	Siła podłączenia (N)	<20
		Siła rozłączenia (N)	<20
Cykle terminacyjne	IEC 352	Ilość cykli	>20
Cykle połączeniowe	IEC 60603-7	Liczba możliwych podłączeń wtyków	>2500
Wibracje	IEC 512-6d	Rezystancja obwodu (mΩ)	<40
Wstrząsy	IEC 512-6c	Zakłócenia kontaktowe (mikrosekundy)	<5
Testy elektryczne		Pomiar	Rezultat
Niski poziom rezystancji obwodu	IEC 512-2a	Rezystancja (mΩ)	<20
Napięcie przebicia dielektryka	IEC 512-4a	1000VAC, 1 minuta	Przeszły
Rezystancja izolacji	IEC 512-3a	Rezystancja (MΩ)	>500
Odporność na korozję w wyniku przepływu gazów mieszanych	IEC 512-11g	Rezystancja obwodu (mΩ)	<40

Żywotność w wysokich temperaturach	IEC 512-9b	Rezystancja obwodu (mΩ)	<40
Wilgotność	IEC 512-11c	Rezystancja obwodu (mΩ)	<40
Szok termiczny	IEC 512-11d	Rezystancja obwodu (mΩ)	<40
Sekwencja klimatyczna	IEC 512-11a	Rezystancja obwodu (mΩ)	<40

2.24 Wymagania dla ekranowanych wtyków RJ45 kat 6A (MPTL)

Minimalne wymagania dla wtyków RJ45

- Zgodność z ISO 11801 Kategoria 6A/Klasa E_A, ANSI/TIA-568.2-D, IEEE 802.3an, ANSI/TIA-1096-A, RoHS;
- Gwarancja pełnego wsparcia PoE i zgodności z wymaganiami IEEE 802.3af i IEEE 802.3at, IEEE 802.3bt (typ 3 i 4) dla aplikacji PoE, PoE+, PoE++ dla minimum 2500 cykli połączeniowych;
- Wsparcie zasilania dla HD-Base-T do 100W;
- Możliwość ponownej terminacji wtyku – min. 20;
- Temperatura pracy: -40°C do +85°C;
- Zgodność z IEC 60603-7;
- Deklaracja zgodności CE;
- Zgodność z UL 1863, UL 2043;
- Klasa szczelności IP20 IEC 60529;
- Fabrycznie wyposażony w zaślepkę przeciw kurzową;
- Wtyk wykonany z cynkowego odlewu ciśnieniowego zapewniający ekranowanie 360° – bez dodatkowych elementów ekranujących dokładanych do wtyku;
- Moduł podczas terminowania ma zapewniać optymalną wydajność poprzez zachowanie geometrii par i zminimalizowanie rozplotu;
- Terminowanie modułu ma zapewniać poprawne umieszczenie przewodników w nożach wykorzystując płynny ruch bez konieczności uderzania w wewnętrzne komponenty modułu;
- Terminowanie wszystkich 4 par w tym samym momencie;
- Wtyk musi mieć prostą konstrukcję, która umożliwia szybkie terminowanie w każdych warunkach i składać się z nie więcej niż 2-óch części;
- Akceptowalna średnica terminowanego kabla: 5,8-9mm
- Dopuszczalna grubość przewodnika dla drutu 22-26AWG;
- Wtyk musi mieć możliwość rozszycia wg. T568A lub T568B;

Wymagane parametry mechaniczne

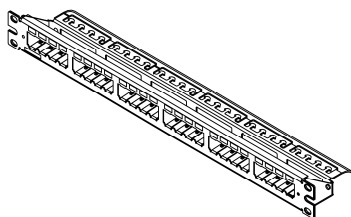
Rodzaj testu	Metoda testu	Jednostka	Oczekiwany typowy parametr
Wibracje	IEC 512-6d	mΩ	<40
Wstrząsy	IEC 512-6c	μs	<5
Trwałość	IEC 512-9a	mΩ	<40
Cykle terminowania	IEC 352		>20
Cykle połączeniowe	IEC 60603-7		>2500

2.25 Wymagania dla ekranowanych paneli krosowych w wersji prostej

Wszystkie kable miedzianego okablowania poziomego należy zakończyć na panelach krosowych prostych o wysokości montażowej 1U i pojemności 24 portów.

Minimalne wymagania dla panelu krosowego 24 porty:

- Wysokość montażowa 1U, wersja prosta, 19”;
- Możliwość numeracji każdego portu u góry panelu;
- Miejsca na opisy portów na górze panelu;
- Maksymalne upakowanie – do 24 portów miedzianych RJ45;
- Panel musi być wyposażony w mechanizmy zatraskowe dla modułów RJ45;
- Montaż i demontaż modułów w panelu musi odbywać się bez specjalistycznych narzędzi;
- Panel krosowy musi umożliwiać także montaż interfejsów multimedialnych na życzenie klienta;
- Panel krosowy musi posiadać z tyłu zintegrowaną półkę dla mocowania i podtrzymywania kabli wraz z możliwością przypięcia pojedynczych kabli opaskami
- Wszystkie porty panelu krosowego muszą mieć automatyczny kontakt z ekranem modułów RJ45;
- Panel musi posiadać wbudowany port dla podłączenia uziemiania;
- Wszelkie porty panelu krosowego, które nie zostaną wykorzystane należy zaślepić zaślepką.



Widok panelu krosowego 24-porty, 1U

Uwaga:

Panele mają być wyposażone w moduły gniazd tego samego typu co w gniazdach dostępowych Użytkownika (PL) ale dodatkowo wyposażone w zaślepkę przeciw kurzową.

2.26 Wymagania dla ekranowanych kabli krosowych miedzianych – wariant 28AWG

Biorąc pod uwagę duże zagęszczenie kabli krosowych należy zastosować kable o zmniejszonym przekroju 28AWG, aby usprawnić zarządzanie, poprawić przejrzystość w szafie, zwiększyć dostęp do portów oraz zoptymalizować przepływ powietrza do urządzeń aktywnych (lepsze chłodzenie).

Minimalne wymagania dla kabli krosowych:

- Kable krosowe mają być wykonane z drutu ekranowanego F/UTP kategorii 6a 28AWG;
- Wymagana maksymalna kable krosowego to 4,7mm;
- Osłona zewnętrzna kabla krosowego CM/LSZH – zgodność z IEC 60332-1, 60754-2, i 61034-2;
- Zgodność z ANSI/TIA-568.2-D, ISO/IEC 11801 Klasa EA, IEC 60603-7, ROHS, deklaracja zgodności CE;

- Obudowa wtyku RJ45 – poliwęglan zgodny z UL94V-0
- Piny wtyków wykonane z poszlacanego fosforobrazu, styki powlekane 50 mikro calami złota dla uzyskania najwyższej wydajności;
- Zgodność z ANSI/TIA-1096-A;
- Konstrukcja wtyku musi uniemożliwiać zaczepianie końcówki kabla krosowego podczas wyciągania go z wiązki kabli;
- Kabel krosowy musi zapewniać identyfikowalność (na kablu musi być etykieta z podaną kategorią kabla, jego długością oraz numerem kontroli jakości);
- Kable krosowe muszą wspierać standardy aplikacji PoE IEEE 802.3af/802.3at (48 kabli w wiązce) oraz 802.3bt typ 3 i typ 4 (24 kable w wiązce);
- Minimalna ilość cykli połączeniowych min. 2500;
- Temperatura pracy: -10°C do 75°C
- Wszystkie kable krosowe mają być fabrycznie wykonane i przetestowane na mapę połączeń oraz NEXT i RL;
- Wszystkie komponenty składowe: wtyki, kabel mają być wyprodukowane i trwale oznaczone przez tego samego producenta co cały system okablowania i zostać objęte 25-letnią gwarancją systemową producenta;
- Należy przewidzieć 100% kabli krosowych do podłączeń z obu stron;
- Kable krosowe muszą opcjonalnie umożliwiać zastosowanie dodatkowych zabezpieczeń uniemożliwiających nieautoryzowane wypięcie kabla z portu;
- Kable krosowe muszą być dostępne w min.8 kolorach;
- Dostępna długość kabli krosowych od 0.2m do 40m;

2.27 Kable światłowodowe wewnętrzne wielomodowe OM4

Okablowanie szkieletowe wewnątrzbudynkowe ma zapewnić kanały transmisyjne o dużej przepływności bitowej łączące poszczególne punkty dystrybucyjne sieci ze sobą. Dobór nośników ma zapewnić minimalizację zakłóceń elektromagnetycznych oraz zapewnienia maksymalnej uniwersalności w uruchamianiu różnorodnych protokołów transmisyjnych. Łąca szkieletowe mają tworzyć topologię gwiazdy.

Poniższa tabela przedstawia zakres wymaganych połączeń światłowodowych pomiędzy punktami dystrybucyjnymi GPD i PPD w obrębie budynku.

Relacja		Przeznaczenie	Ilość kabli	Ilość włókien w kablu	Kategoria włókna	Typ złącza
GPD# 2	PPD_0	LAN	1	12	OM4	LC/PC
GPD# 2	PPD_1	LAN	1	12	OM4	LC/PC
GPD# 2	PPD_2	LAN	1	12	OM4	LC/PC
GPD# 2	GPD_istniejące	LAN	1	12	OM4	LC/PC

2.28 Minimalne wymagania dla kabli OM4

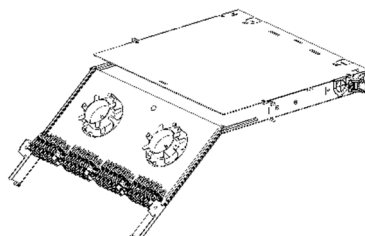
Parametr	Rodzaj kabla
----------	--------------

	24G	
powłoka zewnętrzna kabla – LSZH/LSHF-FR/FRNC	Tak	
konstrukcja ścisłej tuby	PBT	
włókna w buforze	900um	
maksymalna średnica zewnętrzna kabla	8mm	
minimalny promień gięcia podczas instalacji	230mm	
minimalny promień gięcia długoterminowy	115mm	
wszystkie włókna w kablu dla łatwej identyfikacji mają mieć inny kolor	Tak	
Parametry mechaniczne		
Wytrzymałość na rozciąganie (długoterminowe)	1100N	
Wytrzymałość na rozciąganie (podczas instalacji)	3300N	
Wytrzymałość na ściskanie	3000N/100nm	
Parametry środowiskowe		
Temperatura pracy	-20°C do 70°C	-20°C do 70°C
Temperatura instalacji	-40°C do 70°C	-20°C do 70°C
Temperatura przechowywania i transportu	-20°C do 70°C	-20°C do 70°C
Maksymalna tłumienność		
850nm	3.5dB/km	3.5dB/km
1300nm	1.5dB/km	1.5dB/km
Standardy		
Euroklasa	Dca s2 d2 a1	
ISO 11801	Tak	
EN 60794-2-20	Tak	
IEC 60794-2-20	Tak	
EN 50173	Tak	
EN 50290-2-27	Tak	
IEC 60332-1-2	Tak	
IEC 60332-3-24	Tak	
IEC 60754-2	Tak	
IEC 61034	Tak	

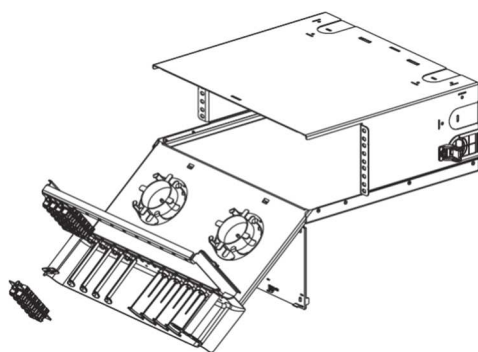
2.29 Opreś światłowodowy

Obudow światłowodow

Obudowy światłowodowe muszą mieć konstrukcję pozwalającą na ochronę, organizację oraz zarządzanie kablami światłowodowymi, spawami, pigtailami, adapterami oraz kablami krosowymi.



Widok obudowy światłowodowej 1U



Widok obudowy światłowodowej 4U

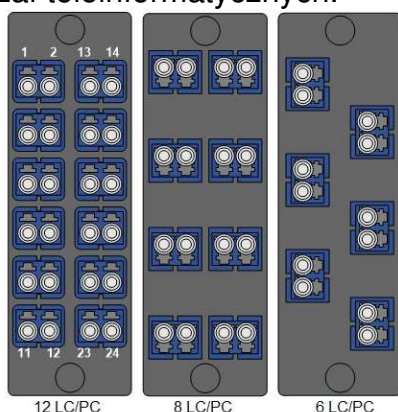
Minimalne wymagania dla obudowy światłowodowej:

- Musi umożliwiać montaż kaset światłowodowych z adapterami ST, SC, LC, MTRJ, E2000, MPO;
- Musi umożliwiać montaż preterminowanych kaset MPO/LC w różnych konfiguracjach;
- Montaż i demontaż kaset w panelu musi odbywać się bez narzędziowo;
- Obudowa światłowodowa musi umożliwiać także montaż interfejsów RJ45 i multimedialnych na życzenie klienta;
- Obudowa musi mieć wysuwaną szufladę ułatwiającą prace instalacyjne;
- Od tyłu obudowa ma posiadać:
 - po każdej stronie do wyboru po 2 wejścia kabli światłowodowych fabrycznie zaślepionych;
 - po każdej stronie możliwość montażu po 2 elementy odciążające (likwidujące naprężenie kabli przy wejściu do obudowy);
 - dla portów wejścia kabli zaślepki z możliwością dostosowania ich do średnicy wprowadzanego kabla światłowodowego;
- Obudowa 1U/19" musi obsłużyć do 4 kaset i 96 włókien dla adapterów LC;
- Obudowa 2U/19" musi obsłużyć do 8 kaset i 192 włókien dla adapterów LC;
- Obudowa 4U/19" musi obsłużyć do 12 kaset i 288 włókien dla adapterów LC;
- Od frontu obudowa musi mieć dodatkowy dystans zabezpieczający przed dostępem do kabli światłowodowych oraz adapterów wraz z uchylną przezroczystą osłoną zamykaną na zamek z możliwością umieszczenia opisów; osłona musi być demontowalna, aby nie przeszkadzała podczas instalacji;
- Od tyłu obudowa musi zostać wyposażona w uchylną osłonę zamykaną na zamek posiadającą pola opisowe; osłona musi być demontowalna, aby nie przeszkadzała podczas instalacji;
- Od frontu obudowa światłowodowa po obu stronach racka musi mieć zamontowane specjalne klipsy sterujące promieniem gięcia oraz uniemożliwiające uszkodzenie kabli krosowych;
- Obudowa 4U musi posiadać w przedniej części poniżej kaset z adapterami min. 8 elementów prowadzących oraz sterujących promieniem gięcia oraz oddzielających poszczególne wiązki kabli krosowych;
- Obudowa światłowodowa ma być fabrycznie wyposażona w dwie demontowalne szpule organizujące zapas włókien światłowodowych wewnątrz obudowy;
- Obudowa światłowodowa ma być fabrycznie wyposażona w elementy organizujące przebieg kabla wewnątrz obudowy;

- Obudowa 1U ma umożliwiać wewnątrz montaż do 4 tacek na 24 spawy światłowodowe;
 - Obudowa 2U ma umożliwiać wewnątrz montaż do 8 tacek na 24 spawy światłowodowe;
 - Obudowa 4U ma umożliwiać wewnątrz montaż do 12 tacek na 24 spawy światłowodowe;
- Wszelkie wolne sloty obudowy światłowodowej, które nie zostaną wykorzystane należy zaślepić zaślepką.

Wymagania dla kaset światłowodowych

Kasety światłowodowe w zależności od potrzeby należy montować w obudowach światłowodowych – należy dokładną lokalizację kaset w obudowach światłowodowych odzwierciedlić na elewacjach szaf teleinformatycznych.



Widok przykładowych kaset światłowodowych z adapterami

Minimalne wymagania dla kaset światłowodowych

- Kasety mają być wyposażona w 6, 8 lub 12 dwuplexowych adapterów LC/PC w zależności od obsługiwanych połączeń;
- Adaptery mają być zgodne z TIA/EIA-568-C.3, TIA/EIA-604 FOCIS-10;
- Adaptery muszą być odpowiednio dobrane kolorystycznie:
 - o dla włókien OM1-OM2 – kolor kremowy;
 - o dla włókien OM3-OM4 – kolor aqua;
 - o dla włókien OM5 – kolor limonkowy;
 - o dla włókien OS1-OS2 – kolor niebieski dla wersji złącz PC
 - o dla włókien OS1-OS2 – kolor zielony dla wersji złącz APC
- Kasea musi być kompatybilna z obudową światłowodową;
- Montaż oraz demontaż kasety nie może wymagać dodatkowych narzędzi;

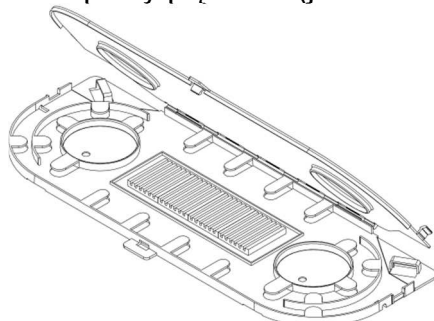
Dodatkowo w ofercie producenta muszą znaleźć się kasety:

- z adapterami ST, SC, LC, MTRJ, E2000, MPO
- obsługujące do 24 włókien na 1 kasetę dla złącz LC;

Wymagania dla tac na spawy światłowodowe

- taca ma obsługiwać do 24 spawów;
- możliwość instalacji osłonek spawów 60mm i 45mm;
- taca ma mieć konstrukcję bez ostrych narożników i krawędzi;
- taca ma mieć zintegrowane elementy do układania zapasu włókien światłowodowych dbając o zachowanie odpowiednich promieni gięcia;

- taca musi posiadać uchwyty zabezpieczające przed wypadaniem włókien z tacy;
- taca musi być wyposażona w zamykaną przezroczystą osłonę, na zawiasach która chroni włókna i spawy światłowodowe;
- możliwość instalacji tac na spawy piętrowo (jedna na drugą);



Widok tacy na spawy światłowodowe

Wymagania dla piguli światłowodowych OM4 LC

Światłowod piguła LC musi spełniać wymagania:

- osłona zewnętrzna – LSZH;
- kolor osłony: aqua
- średnica zewnętrzna – 900um

Parametry środowiskowe

- Temperatura pracy: 0°C do 60°C
- Temperatura przechowywania i transportu: -40°C do 70°C

Parametry optyczne IL: max. 0,15dB

Parametry optyczne RL: min. 26dB

Trwałość łączy

- Min. 500 cykli połączeniowych;

Normy

- ISO/IEC 11801, TIA/EIA-568-C.3, TIA-604-3 (FOCIS-3), TIA-604-10 (FOCIS-10), IEC 60332-1-2, IEC 60332-3-24, IEC, 60754-1, IEC 60754-2, IEC 61034-2, RoHS

Wymagania dla kabli krosowych światłowodowych OM4 LC-D

Światłowod kabl krosowy LC duplex musi spełniać wymagania:

- osłona zewnętrzna – LSZH;
- kolor osłony: aqua
- rodzaj kabla: pojedyncza okrągła osłona z 2-oma włóknami światłowodowymi;
- średnica zewnętrzna – 2mm
- długość kabli krosowych co 1m w zakresie od 1m do 50m;
- minimalny promień gięcia kabla długoterminowo: 40mm
- minimalny promień gięcia kabla krótkoterminowo: 20mm
- konstrukcja złącza LC duplex wraz z osłoną złącza musi umożliwiać łatwe odłączenie złącza LC od adaptera LC poprzez pociągnięcie za osłonę złącza (boota); takie rozwiązanie jest bardzo przydatne przy dużym zagęszczeniu portów LC z racji na małe gabaryty tego złącza i trudny dostęp; rozwiązanie takie nie może powodować uszkodzenia złącza ani kabla światłowodowego;
- konstrukcja złącza LC duplex wraz z osłoną złącza musi umożliwiać łatwą zmianę polaryzacji złącza poprzez zdjęcie i odwrócenie obudowy złącza;

Parametry środowiskowe

- Temperatura pracy: -10°C do 60°C
- Temperatura przechowywania i transportu: -40°C do 70°C

Parametry optyczne IL: max. 0,1dB

Parametry optyczne RL: min. 26dB

Trwałość złączy

— Min. 500 cykli połączeniowych;

Normalizacja

— ISO/IEC 11801, TIA/EIA-568-D.3, TIA-604-10 (FOCIS-10), RoHS

2.30 Punkty dystrybucji okablowania strukturalnego

W szafach dystrybucyjnych będzie instalowany osprzęt połączeniowy pasywny oraz sprzęt aktywny w różnych konfiguracjach. W zależności od tego co będzie znajdowało się w szafie należy dobrać jej odpowiednią konstrukcję i tak:

- mieszane wyposażenie czyli elementy pasywne, switchy aktywne oraz serwery i inne urządzenia – należy dobrać szafę o konstrukcji uniwersalnej dostosowanej do obsługi wszelkich elementów; szafa taka powinna zapewniać sprawne zarządzanie dużą ilością połączeń zarówno od strony kabli przychodzących jak i patchcordów, dobry przepływ powietrza dla chłodzonych urządzeń oraz dostęp do zasilania które nie koliduje z okablowaniem logicznym. Warto rozważyć w niektórych przypadkach zastosowanie otwartych konstrukcji rackowych z kanałami bocznymi do zarządzania okablowaniem – konstrukcje takie są idealne do stosowania w miejscach o ograniczonej powierzchni;

Szafy oraz wszelkie akcesoria do nich (organizery, zaślepki, listwy zasilające PDU) muszą pochodzić z oferty tego samego producenta co okablowanie strukturalne.

2.31 Wymagania dla szaf stojących w serwerowni o konstrukcji uniwersalnej

- Zgodność ze standardem: EIA-310-E / TIA/EIA-942
- Wysokość 42U,
- Szerokość 800mm,
- Głębokość 1000mm,
- Obudowa szafy wykonana z zespawanej i zmontowanej konstrukcji stalowej,
- Wytrzymałość statyczna min. 1500kg na nóżkach i 500kg na kółkach (opcja),
- Wszystkie 4 profile / słupy montażowe o rozstawie 19" muszą umożliwiać regulację w przód i w tył tak aby umożliwić montaż sprzętu zarówno sieciowego jak i serwerowego; wewnątrz szafy musi znajdować się podziałka umożliwiająca precyzyjne ustawienie szyn w pionie,
- Słupy montażowe muszą posiadać oznaczenia każdego U w szafie aby ułatwić planowanie i montaż urządzeń,
- Konstrukcja szafy o szerokości 800mm musi umożliwiać pionowy montaż w przestrzeni bocznej między rakiem a ścianą szafy paneli krosowych 19"- minimalne wymagane upakowanie paneli 19" – 4 sztuki ,
- Drzwi przednie wypukłe jednoskrzydłowe z perforacją min.69% z dwustopniowym zamkiem i klamką,
- Drzwi tylne dwuskrzydłowe z perforacją min.69% z trójstopniowym zamkiem i klamką,
- W szafach panele boczne dzielone poziomo muszą zapewniać swobodny dostęp do urządzeń,
- Wszystkie elementy rozłączne tj. drzwi, ściany boczne itd. mają posiadać linki uziemiające,
- W dachu muszą znajdować się otwory z zaślepkami z włókniną umożliwiające wprowadzenie kabli:

- min. 4 otwory w szafach o szerokości 800mm
- Szafa ma posiadać uchwyt do montażu minimum dwóch pionowych listw PDU o pełnej wysokości,
- Szafa musi umożliwiać montaż z tyłu min. dwóch listw PDU o pełnej wysokości na jednej stronie szafy,
- Szafa ma posiadać nóżki regulowane, z możliwością wypoziomowania szafy,
- Szafa ma być dostępna w kolorze RAL 9005 oraz RAL 9003;
- Szafa musi umożliwiać tworzenie zamkniętych korytarzy (kiosk);
- Szafy wyposażać w pionowe organizery kabli krosowych typu finger, które nie zajmują powierzchni montażowej w szafie;
- Organizery kabli zamontować na całej wysokości szafy po obu stronach;

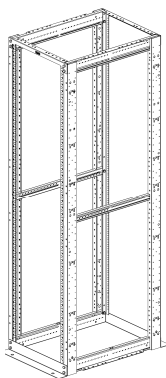
2.32 Wymagania dla Rack 4-słupowy – pomieszczenia PPD

Otwarty stelaż Rack 19" wyposażony w ramę 4-słupową, musi spełniać standard EIA/ECA-310-E oraz mieć następujące wymiary:

- Max. 45U; 2134x591x584mm (WxSxG)

Stelaż musi spełniać poniższe wymagania i funkcjonalności:

- umożliwiać regulację szyn montażowy tylnych i przednich;
- obciążenie statyczne min. 1134kg;
- szyny montażowe muszą posiadać oznaczenie każdego U oraz umożliwiać montaż w taki sposób aby numeracja zaczynała się od góry lub od dołu racka;
- przednie i tylne słupy montażowe stelaża muszą umożliwiać montaż pionowych prowadnic kabli (patrz pionowych menedżerów kabli);
- maksymalnie 2 punkty uziemienia;
- przednie i tylne słupy montażowe stelaża muszą umożliwiać montaż akcesoriów takich jak:
 - pionowe i poziome listwy zasilające PDU;
 - elementy organizacyjne dla zapasu kabli krosowych;
 - adaptory do montażu elementów 0U;
 - dukty termiczne umożliwiające doprowadzenie chłodnego powietrza do urządzeń z przepływem bocznym;
 - pionowe panele zaślepiające;
- umożliwiać montaż opcjonalnych kółek montowanych do podstawy stelaża;



Widok Racka 4-słupowego

2.33 Listwy zasilające PDU i monitoring środowiskowy

Listwy PDU

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

Tabela listw PDU stosowanych w projekcie

Szafa	Poziom monitorowania	Ilość PDU	Ilość faz w PDU	Prąd wejściowy na fazę	Listwa pionowa/pozycja	Moc pozorna	Gniazda C13 – minimalna wymagana ilość	Gniazda C19 – minimalna wymagana ilość
GPD#1	MP	1	1	32A	pionowa	7,4(kVA)	20	4
GPD#2	MP	1	1	32A	pionowa	7,4(kVA)	20	4
GPD#3	MP	1	1	32A	pionowa	7,4(kVA)	20	4
GPD#4	MP	1	1	32A	pionowa	7,4(kVA)	20	4
PPD 0	MP	1	1	16A	pionowa	3,7(kVA)	8	0
PPD 1	MP	1	1	16A	pionowa	3,7(kVA)	8	0
PPD 2	MP	1	1	16A	pionowa	3,7(kVA)	8	0

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

- Zgodność z normami:
 - o ANSI/TIA-569-D Telecommunications Pathways and Spaces, 2015;
 - o ANSI/NFPA 70 – National Electric Code, 2008, 2014;
 - o 2014/35/EU – Low Voltage Directive;
 - o 2014/30/EU – Electromagnetic Compatibility Directive;
 - o 2011/65/EU – Restriction of use of certain hazardous substances in electrical and electronic equipment directive (RoHS2);
 - o EN 55032:2015 – Information technology equipment. Radio disturbance characteristics. Limits and method of measurement;
 - o EN 55024:2010 – Information technology equipment. Immunity characteristics. Limits and methods of measurement;
 - o EN 60950-1: 2006/A11:2009/A1:2010/A12:2011/A2:2013 – Information technology equipment. Safety. General requirement;
 - o EN 50600-2-2: Data Center Electrical Power Distribution;
- Certyfikat - FCC Rules Part 15 – EMC Verification, Canadian ICES-003;
- Producent musi oferować listwy PDU zarówno w wersji montażu pionowej jak i poziomej 19”;
- PDU muszą wytrzymać temperaturę do 60°C przy pełnym obciążeniu na wszystkich gniazdach;
- PDU o dużej gęstości upakowania gniazd (do 48 sztuk) na jednym profilu o wymiarach max. 1821.2mm x 50.8mm x 111.8mm (musi zmieścić się do szafy 42U) dla zminimalizowania przestrzeni i zmaksymalizowania przepływu powietrza w szafie;
- Szerokość listw pionowych max. 50,8mm;
- Możliwość wymiany kontrolera z wyświetlaczem w trakcie pracy listwy PDU (Hot-Swap);

- Kontroler PDU z wyświetlaczem musi mieć możliwość obrotu o 180° w zależności od strony na której jest montowana listwa;
- Kontroler musi posiadać jasny wyświetlacz OLED z wysokim współczynnikiem kontrastu;
- Redundantny dostęp sieciowy 1Gb/s w konfiguracji 2N dla redundancji połączeń w sieci lub połączeniu do sieci różnych użytkowników;
- Przełączanie gniazd zasilających i krytycznych funkcji PDU musi odbywać się za pośrednictwem HTTPS/TLS, a nie SSL;
- Musi być obsługiwane bezpieczne monitorowanie sieci, aby uniknąć wtargnięć - cała komunikacja danych powinna obsługiwać bezpieczne funkcje RESTful API przez HTTPS/TLS z wykorzystaniem otwartego, niezastrzeżonego standardu branżowego;
- Musi obsługiwać standard Redfish API;
- Gniazda zasilające muszą obsługiwać najnowsze zabezpieczenia i spełniać rygorystyczne wymagania bezpieczeństwa narzędzi do skanowania:
 - HPE WebInspect Security;
 - Tenable Nessus;
 - DDI Frontline;
 - BackTrack Linux Security Editor;
- PDU musi obsługiwać kodowane oznaczone kolorami gniazda C13/C19 w celu identyfikacji każdej z 3 faz z kolorowymi bezpiecznikami automatycznymi;
- PDU musi być dostępne przynajmniej w 6 kolorach do wyboru w celu łatwej identyfikacji i zarządzania zasilaniem w szafach;
- PDU musi obsługiwać połączenie sieciowe 1Gb/s i umożliwiać połączenie do 4 listw PDU w celu oszczędzania adresów IP;
- Montaż listw PDU musi odbywać się bez użycia narzędzi i umożliwiać regulowanie położenia jednostki PDU;
- Graficzny interfejs użytkownika jednostki PDU musi dostosowywać się do rozdzielczości ekranu urządzenia użytkownika w celu uzyskania optymalnego interfejsu na urządzeniach mobilnych i tabletach;
- Kodowane gniazda IEC są kompatybilne z bezpiecznymi kablami zasilającymi z blokowaniem W i V z dodatkowym zabezpieczeniem za pomocą standardowych opasek kablowych;
- Minimum 3-letnia standardowa gwarancja producenta z możliwością rozszerzenia do 5-lat;
- Skalowalność pod względem zarządzania urządzeniem za pomocą lokalnego serwera WWW do systemu DCIM w celu monitorowania energii i mocy u jednego dostawcy;
- Obsługa portu USB umożliwiającego szybkie instalowanie oprogramowania wbudowanego i poprawek zabezpieczeń bez wyłączenia niezgodnych urządzeń w sieci;
- Musi istnieć możliwość wyłączenia portu USB do udostępniania za pomocą blokady programowej w celu ochrony przed włamaniami;
- Monitorowanie zużycia energii z dokładnością do +/-1% zapewniające dokładność rozliczeniową zgodnie ze specyfikacjami IEC;
- Pomiar musi obejmować odczyty V, A, VA, W, kWh i PF;
- Obsługa wysokiej niezawodności hydrauliczno-magnetycznych wyłączników awaryjnych stabilnych w temperaturze do min.60°C;

- Oferowany asortyment listw PDU musi zawierać możliwość elastycznego zastosowania odpowiedniej listwy w zależności od potrzeb klienta m.in.:
 - Niemonitorowanych listw (NM);
 - Monitorowane Wejścia (MW) - jednostka PDU z możliwością monitorowania potencjalnej agregacji mocy po to aby szybko zidentyfikować potencjalne problemy z zasilaniem i odzyskać dostępną lub niewykorzystaną moc;
 - Monitorowane Przełączanie (MP) – jednostka PDU z możliwością monitorowania potencjalnej agregacji mocy i przełączania poziomu wyjściowego na poszczególne gniazda lub grupę gniazd. Umożliwia sekwencjonowanie mocy, ponowne uruchomienie sprzętu lub ograniczenie nieuprawnionego użycia gniazda zasilającego;
 - Monitorowanie na poziomie indywidualnego Gniazda (MG) – jednostka PDU z możliwością monitorowania mocy wyjściowej, aby szybko zidentyfikować potencjalne problemy z zasilaniem oraz odzyskać dostępną lub niewykorzystaną moc wyjściową na poziomie gniazd, umożliwiając ponowne przegrupowanie lub wyłączenie poszczególnych serwerów w celu odzyskania dostępnej lub niewykorzystanej mocy;
 - Monitorowanie i Przełączanie na poziomie indywidualnego Gniazda (MPG) – jednostka PDU z możliwością monitorowania mocy wyjściowej i możliwości przełączania poziomu wyjściowego dla poszczególnych gniazd lub grupy gniazd. Monitorowanie mocy na poziomie indywidualnego gniazda zapewnia praktyczne dane dotyczące zarządzania zużyciem energii każdego podłączonego urządzenia IT, umożliwiając ponowne przegrupowanie lub wyłączenie poszczególnych serwerów w celu odzyskania dostępnej lub niewykorzystanej mocy;
- Spełnia globalne standardy zgodności zasilania: UL, cULus, CE i EAC;
- Obsługa monitorowania rozgałęzionych obwodów i równoważenia obciążenia każdego obwodu;
- Obsługa gniazd naprzemiennych;
- Wyświetlanie wszystkich trzech faz jednocześnie na wyświetlaczu OLED podczas ręcznego gromadzenia danych;
- PDU musi natywnie obsługiwać różne czujniki i rozwiązania kontroli dostępu za pośrednictwem tej samej jednostki PDU bez zewnętrznego urządzenia bramowego;
- Dostawca PDU musi dostarczać cyfrowe czujniki środowiskowe oraz bezpieczeństwa m.in.:
 - Temperatury;
 - Temperatury + wilgotności;
 - 3x temperatura + wilgotność;
 - Liniowy czujnik zasilania;
 - Punktowy czujnik zasilania;
 - Wejście styku bez potencjałowego;
 - Kontaktron drzwiowy;
 - HUB dostępowy dla kontroli dostępu do szafy (wymagana obsługa technologii kart 125kHz i 13,56MHz);
 - Listwa oświetleniowa LED;
 - HUB rozszerzenia portów sensorów
- Obsługa interfejsu bezprzewodowego za pomocą klucza sprzętowego sieci bezprzewodowej;

Parametry elektryczne listw PDU

Napięcie wejściowe	Jednofazowe PDU – 240V
Prąd wejścia (na fazę)	16A 32A
Moc wejściowa	3,7- 7,4 (kVA)
Częstotliwość wejściowa	50/60Hz
Napięcie wyjściowe	120-240VAC
Maksymalny prąd wyjściowy (gniazdo)	IEC C13: 10A IEC C19: 16A NEMA 5-20R: 16A
Zabezpieczenie przed przeciążeniem (jeśli dotyczy)	Zabezpieczenia hydrauliczno-magnetyczne

Parametry ogólne listw PDU

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

2.34 Monitoring środowiska

Czujniki temperatury i wilgotności

Czujniki powinny zawierać:

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

Czujniki temperatury i wilgotności musi być zgodny z następującą specyfikacją: wybierz odpowiedni rodzaj stosowanych czujników

	Temperatura	Temperatura i wilgotność	3x temperatura i wilgotność
Elektryczne			
Napięcie robocze	5V DC	5V DC	5V DC
Skala	0°C~+65°C, wilgotność względna 10–90%, bez kondensacji	0°C~+65°C, wilgotność względna 10–90%, bez kondensacji	0°C~+65°C, wilgotność względna 10-90%, bez kondensacji
Precyzja	±2°C	±2°C	±2°C
	±5% RH w 5-50°C	±5% RH w 5-50°C	±5% RH w 5-50°C
	10 ~ 90% RH	10 ~ 90% RH	10 ~ 90% RH
Typ przewodu (od PDU do puszki czujnika)	Patchcord kat. 5, UTP	Patchcord kat. 5, UTP	Patchcord kat. 5, UTP
Fizyczne			
Długość	2m	2m (od PDU do puszki czujnika)	2m (od PDU do puszki czujnika)
		1m (czujnik temperatury T1/T3 do puszki czujnika)	1m (czujnik temperatury T1 / T3 do puszki czujnika)
Środowiskowy			

Wyokość p.m. (klopoty/ prhowywy)	0- 3048m/0-15240m	0-3048m/0-15240m	0-3048m/0-15240m
Temperatur (Obług/ prhowywy)	0°C~+70°C/-20~+70°C	0°C~+70°C/-20~+70°C	0°C~+70°C/-20~+70°C
Wilgotność (Obług/ prhowywy)	0-95% RH, bez kondensacji	0-95% RH, bez kondensacji	0-95% RH, bez kondensacji
Spłł			
Wryfikj środowkow	ROHS, WEEE	ROHS, WEEE	ROHS, WEEE

Czujnik

Czujnik służy do monitorowania stanu wody z przodu szafy lub w innym potencjalnym miejscu wycieku wody i powinien zawierać:

- Bezpośrednie połączenie z PDU za pomocą dostarczonego standardowego kabla sieciowego;
- Kompaktowe urządzenie odpowiednie do wielu lokalizacji;
- Liczba czujników na szafę lub rząd i CARC - ?

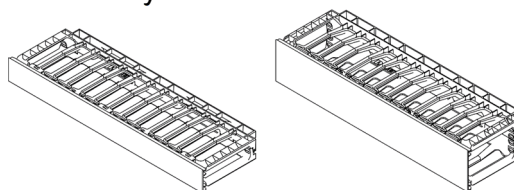
Czujnik zalania musi spełniać następujące wymagania:

Czujnik	
Elektry	
Napię i robo	5V DC
Skł	Ciecze o rezystancji <2 MΩ na cm
Fi y	
Długość k bła:	5m
Typ drutu:	Patchcord kat. 5, UTP
Środowko	
Wyokość p.m. (klopoty/prhowywy)	0-3048m / 0-15240m
Temperatur (klopoty/prhowywy)	0°C~+65°C /-20~+70°C
Wilgotność (klopoty/prhowywy)	10 - 95% RH, bez kondensacji (praca)
Spłł	
Wryfikj środowkow	ROHS, WEEE

2.35 Organi j k bli w fi

Organi ry poziom j do tro

Wszystkie projektowane szafy muszą zostać wyposażone w organizery poziome z pokrywą (możliwość otwarcia góra/dół) zabezpieczającą przed wypadaniem kabli krosowych. Organizery poziome mają mieć wysokość 1U i/lub 2U i przynajmniej po 13 wejść z góry i z dołu na kable krosowe. W tylnej części organizera mają znajdować się przynajmniej 2 wyloty owalne na wyprowadzenie kabli krosowych do tyłu; krawędzie wylotów muszą być zabezpieczone w taki sposób aby kable krosowe nie były narażone na ostre krawędzie. Pojemność organizera musi zostać dobrana w taki sposób aby obsłużyć projektowaną ilość i rodzaj kabli krosowych wraz z min.50% zapasem przestrzeni na przyszłość. Skrajne boczne prowadnice kablowe muszą mieć kształt zapewniający odpowiedni promień gięcie kabli krosowych oraz nie narażać ich na ostre krawędzie.



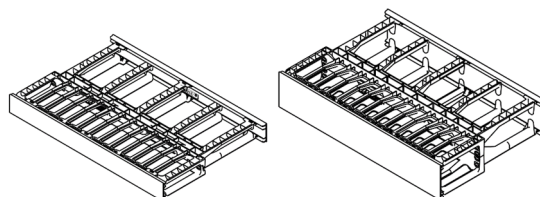
Widok poziomego organizera jednostronnego 1U i 2U 19"

Wymagana minimalna pojemność kabli krosowych w menadżerach poziomych jednostronnych

Wyokość	Złoty wypłiki kabli krosowymi (30%)				Mikymł wypłiki kabli krosowymi (50%)			
	Pród młdżr							
	Kł.6A (28AWG - 4,7mm)		Kł.6A (24AWG - 6,99mm)		Kł.6 (28AWG - 3,81mm)		Kł.6 (24AWG - 5,97mm)	
2U	109	182	49	82	166	277	67	112

Organy poziom dwustronny

Wszystkie projektowane szafy muszą zostać wyposażone w organizery poziome dwustronne z pokrywami (możliwość otwarcia góra/dół) zabezpieczającymi przed wypadaniem kabli krosowych. Organizery poziome mają mieć wysokość 1U i/lub 2U i przynajmniej 13 wejść z góry i z dołu na kable krosowe. W środkowej części organizera mają znajdować się przynajmniej 2 wyloty owalne na wyprowadzenie kabli krosowych do tyłu; krawędzie wylotów muszą być zabezpieczone w taki sposób aby kable krosowe nie były narażone na ostre krawędzie. Pojemność organizera musi zostać dobrana w taki sposób aby obsłużyć projektowaną ilość i rodzaj kabli krosowych wraz z min.50% zapasem przestrzeni na przyszłość. Skrajne boczne prowadnice kablowe muszą mieć kształt zapewniający odpowiedni promień gięcie kabli krosowych oraz nie narażać ich na ostre krawędzie.



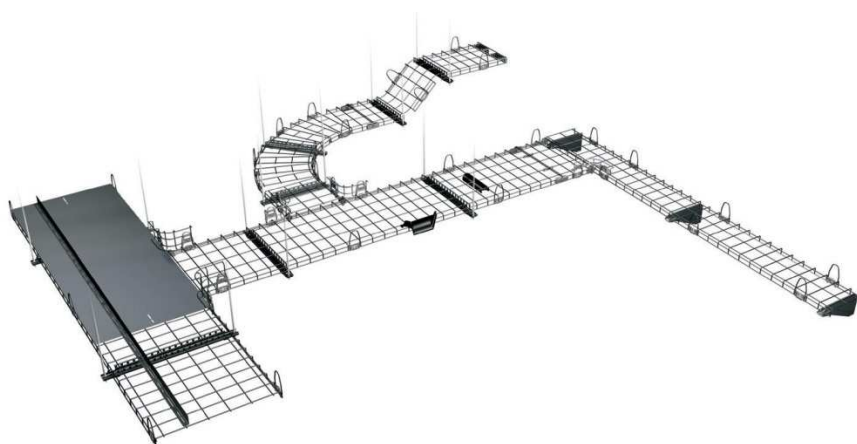
Widok poziomego organizera dwustronnego 1U i 2U 19"

Wymagana minimalna pojemność kabli krosowych w menadżerach poziomych jednostronnych

Wyokość	Złoty wypłiki kabli (30%)								Mikymł wypłiki kabli (50%)							
	Pród młdżr								Tył młdżr							
	Kł.6A (28AWG - 4,7mm)	Kł.6A (24AWG - 6,99mm)	Kł.6 (28AWG - 3,81mm)	Kł.6 (24AWG - 5,97mm)	Kł.6A (28AWG - 4,7mm)	Kł.6A (24AWG - 6,99mm)	Kł.6 (28AWG - 3,81mm)	Kł.6 (24AWG - 5,97mm)	Kł.6A (28AWG - 4,7mm)	Kł.6A (24AWG - 6,99mm)	Kł.6 (28AWG - 3,81mm)	Kł.6 (24AWG - 5,97mm)	Kł.6A (28AWG - 4,7mm)	Kł.6A (24AWG - 6,99mm)	Kł.6 (28AWG - 3,81mm)	Kł.6 (24AWG - 5,97mm)
2U	109	182	49	82	166	277	67	112	123	206	55	93	188	314	76	127

2.36 Trasy kablowe dla połączeń między i światłowodowych w Serwerowni

System metalowych siatkowych koryt kablowych to konfiguracja umożliwiająca rozprowadzenie wiązek kabli miedzianych i światłowodowych do szaf i pomiędzy szafami w pomieszczeniach dedykowanych dla punktów dystrybucji okablowania i Serwerowniach. Projektowane rozwiązanie znacznie skraca czas instalacji, poprawia zarządzanie kablami i zwiększa bezpieczeństwo użytkownika.



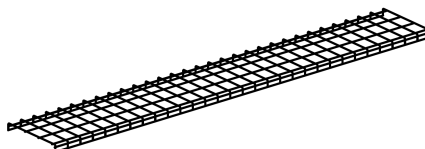
Przykład systemu tras dla kabli miedzianych

System kanałów kablowych dla kabli miedzianych musi umożliwiać instalację na tych samych uchwytych co system koryt kablowych dla kabli światłowodowych.

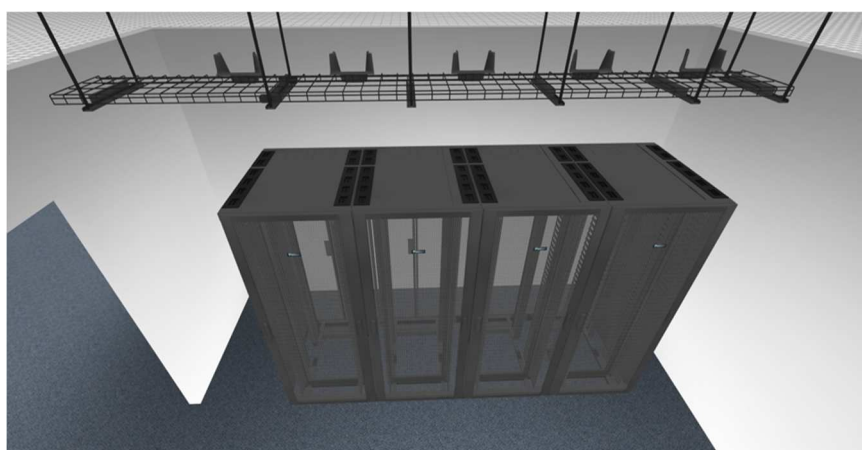
2.37 Minimalny wymóg dla systemu i-tkowyh koryt m-tlowyeh

Zaprojektowana konstrukcja koryta kablowego nie posiada integralnych ścian bocznych co eliminuje potrzebę docinania koryt w miejscach:

- skrzyżowań koryt,
- wodospadów kablowych (miejsca wyprowadzenia kabli z koryta do szaf),
- zmian kierunku (poziomych i pionowych) trasy kablowej.



Widok koryta kablowego



Widok koryt w serwerowni

Wszelkie akcesoria dodatkowe do systemu koryt kablowych takie jak:

- ograniczniki boczne uniemożliwiające wypadanie wiązek kablowych z koryta,
- elementy zapewniające odpowiedni promień gięcia kabli na skrzyżowaniach,
- wodospady kablowe,

muszą być montowane bez użycia dodatkowego sprzętu i narzędzi na tzw. szybki zatrzask.

Ograniczniki boczne muszą mieć możliwość wymiany na wyższe, aby dostosować się do przyszłych zmian np. większa ilość wiązek kablowych.

Łączniki stosowane do połączeń koryt kablowych muszą mieć zintegrowaną śrubę, która po złączeniu 2-óch elementów koryt dokręcana wcina się w metal zapewniając odpowiednie połączenie elektryczne pomiędzy nimi co zapewnia odpowiedni poziom bezpieczeństwa podczas uziemiania systemu koryt.

System koryt kablowych musi umożliwiać tworzenie wielopoziomowych struktur dla prowadzenia w osobnych kanałach np.:

- kabli miedzianych logicznych,
- kabli światłowodowych,
- kabli zasilających,

a także, musi mieć możliwość integracji z dedykowanym systemem duktów światłowodowych przeznaczonych tylko dla połączeń optycznych.

System koryt kablowych musi być dostosowany swoim rozmiarem do instalacji zapewniając odpowiednią pojemność dla wszystkich wiązek połączeniowych realizowanych podczas instalacji +50% zapasu na przyszłą rozbudowę.

Instalowane rozwiązanie musi mieć możliwość instalacji na:

- szpilkach montowanych do sufitu,
- uchwytach montowanych do ściany,
- uchwytach montowanych na dachu szafy;

Wymaga się, aby system umożliwiał zastosowanie koryt o szerokości od 20cm do 76cm w zależności od zapotrzebowania ilościowego oraz obciążenia.

2.38 Obciążenie koryt kablowych

Obciążenie koryt kablowych musi być zgodne z normą EN 61537:2007 – uwzględnia ona różne konfiguracje tras, takie jak skrzyżowania typu T, skrzyżowania typu X, odcinki proste i odcinki proste łączone.

Instalowany system koryt kablowych nie może być zależny od wysokości ścian bocznych. Wszelkiego rodzaju połączenia systemu koryt nie mogą naruszać fabrycznej struktury koryta (z wyłączeniem skracania długości koryta) co wpływa na zmniejszenie ogólnej wytrzymałości trasy kablowej.

2.39 Uziemienie systemu koryt

Projektowany system koryt kablowych należy uziemić zgodnie z normą EN 50310

2.40 System zarządzania listwami zasilającymi PDU oraz monitoringiem środowiskowym

Oprogramowanie musi być rozwiązaniem holistycznym, zarządzającym i monitorującym:

- porty paneli krosowych miedzianych i światłowodowych – opcjonalny moduł do wykorzystania w przyszłości,
- porty przełączników sieciowych – opcjonalny moduł do wykorzystania w przyszłości,
- listwy zasilające PDU,

- sensory monitorujące środowisko,
- monitoring zasobów IT – opcjonalny moduł do wykorzystania w przyszłości,

Pozwoli to na pełną identyfikację ryzyka związaną z połączeniami sieciowymi, zajętością przestrzeni w szafach, dostępnością energii elektrycznej dla urządzeń, czy też panujących warunków otoczenia (np.; temperatury i wilgotności), czy również stanu otwarcia drzwi lub klamek szaf.

2.41 Minimalne oczekiwana funkcjonalność oprogramowania

- **Pomiar zużycia energii oraz monitoring środowiska** – system musi zapewniać pomiar poziomów mocy i atrybutów środowiskowych w określonym czasie w celu poprawy zarządzania systemem i niezawodności. Platforma oprogramowania musi zawierać wszystkie funkcje związane z zarządzalnymi listwami dystrybucji zasilania (PDU), czujnikami środowiskowymi i kontrolą dostępu do szaf. Obejmuje to monitorowanie mocy i środowiska, funkcje administracyjne (np. ustawianie parametrów progów alarmowych) oraz raporty dotyczące mocy / środowiska. System musi monitorować i katalogować wydajność i zużycie energii w środowiskach informatycznych, umożliwiając tworzenie trendów i analiz w celu poprawy wydajności;
 - **Pomiar i monitoring mocy** – system musi mierzyć i wyświetlać zużycie energii w czasie rzeczywistym na poziomie gniazda i POU (szafy) oraz identyfikować problemy związane z zasilaniem, pomagając efektywnie zarządzać wykorzystaniem mocy, ograniczać ryzyko i zapobiegać przestojom związanym z zasilaniem;
 - **Pomiar i monitorowanie środowiska** – system musi mierzyć i wyświetlać warunki środowiskowe, takie jak wilgotność i temperatura, przepływ powietrza w urządzeniach lub na poziomie szafy / racka, i zapewniać alarmy, jeśli progi środowiskowe są przekroczone, umożliwiając podjęcie działań zapobiegających przegrzaniu sprzętu i nieprawidłowemu działaniu;
 - **Wizualizacja trendów danych** – system musi umożliwiać użytkownikom obserwowanie trendów poziomów mocy i atrybutów środowiskowych w określonych okresach, aby pomóc zrozumieć czynniki, które mogą mieć wpływ na optymalną wydajność i wydajność;
 - **Dokumentacja wykorzystania mocy i ciepła** – system musi wykorzystywać kompleksową, dobrze zorganizowaną relacyjną bazę danych do dokumentowania i raportowania wykorzystania mocy, poziomów temperatury i wilgotności, ułatwiając szybsze odzyskiwanie rekordów i wspomagając planowanie rozbudowy;
 - **Zaawansowany pulpit nawigacyjny i raporty**
Platforma oprogramowania musi korzystać z predefiniowanych i niestandardowych pulpitów nawigacyjnych i raportów, aby zapewnić wgląd w kluczowe wskaźniki operacyjne infrastruktury informatycznej przedsiębiorstwa. W połączeniu z różnymi modułami oprogramowania, użytkownik współdzieli wgląd we wszystkie aspekty infrastruktury fizycznej, aby efektywnie i wydajnie zarządzać swoimi zasobami.

Pulpity dashboardów platformy oprogramowania muszą przy użyciu funkcji typu przeciągnij i upuść zapewniać wgląd we wskaźniki operacyjne, które obejmują kluczowe parametry potrzebne do zarządzania całą infrastrukturą IT - zasilanie, przestrzeń, połączenia i śledzenie zasobów - za pośrednictwem szeregu wstępnie zdefiniowanych pulpitów nawigacyjnych.

Użytkownicy muszą mieć możliwość definiowania niestandardowych raportów i pulpitów nawigacyjnych przy użyciu szerokiego wachlarza elementów wizualizacji danych, takich jak mierniki, wykresy i tarcze. Raporty powinny zapewniać wgląd w aktywność użytkowników, wydajność systemu i najczęściej używane raporty.

Oprogramowanie musi zawierać zestaw predefiniowanych raportów i pulpitów nawigacyjnych z zaawansowaną wizualizacją, obejmującą następujące aspekty:

- Zasilanie i środowisko;

2.42 Urządzenia sieciowe LAN

Założenia ogólne:

Struktura sieci lokalnej i jej topologia, odzwierciedla wymaganą strukturę na potrzeby dostarczenia odpowiedniej jakości usług sieciowych, dla systemów Security i innych, między innymi:

- bezpiecznego dostępu dla użytkowników końcowych,
- systemów telefonii, działających na protokole IP,
- dostępu gościnnego dla użytkowników zdefiniowanych, w ramach polityki bezpieczeństwa, zunifikowanego dla dostępu przewodowego, jak i bezprzewodowego,
- systemów bezpiecznego dostępu do sieci Internet lub/i instytucji zewnętrznych (w celu realizacji systemów backupowych, dostępu do sieci Internet itp.).

Powyższe zapewnione jest nie tylko na podstawie odpowiedniej architektury sieci lokalnej, ale również innych systemów i aplikacji, mających wspierać realizację zunifikowanego, a zarazem bezpiecznego dostępu do sieci komputerowej, na której pracować będą różne systemy i aplikacje, mające rozdzielne funkcjonalności. Zaprojektowana infrastruktura sieciowa musi zapewniać jednolitą platformę sprzętową i programową, w pełni ze sobą zintegrowaną, zapewniającą późniejsze jednolite utrzymanie sieci, jej rekonfigurację i modyfikacje, na potrzeby realizacji potrzeb systemów i aplikacji. Aby zagwarantować pełną kompatybilność całego systemu wszystkie jego komponenty muszą pochodzić od jednego producenta. Zapewni to jeden punkt zgłaszania ewentualnych usterek bądź problemów konfiguracyjnych oraz spójne warunki świadczenia gwarancji oraz wsparcia serwisowego. Najistotniejszym założeniem zaprojektowanej sieci komputerowej, jest jej pełna unifikacja, zarówno w zakresie sieci przewodowej, jak i bezprzewodowej, z uwzględnieniem jednolitych mechanizmów zarządzania punktami dostępu do sieci, kontroli dostępu do sieci, w oparciu o systemy NAC. Jedynie styk z siecią Internet lub sieciami zewnętrznymi, zakłada się, że może być zarządzany i konfigurowany osobno, ale z uwzględnieniem współpracy z siecią LAN. Zaletą takiej struktury jest, uwzględnienie osobnych mechanizmów bezpieczeństwa na styku pomiędzy sieciami (lokalną i sieciami zewnętrznymi), z uwzględnieniem odpowiedniej separacji i poziomu bezpieczeństwa

systemów i aplikacji.

W dalszej części opisu, przedstawione są szczegóły związane z architekturą sieci lokalnej, zarówno przewodowej, jak i bezprzewodowej, wymagania, związane z realizacją poszczególnych warstw sieci lokalnej i zastosowanych urządzeń. Należy zwrócić uwagę, że przedstawione wymagania, są wymaganiami minimalnymi, w celu realizacji bądź umożliwienia w przyszłości podłączenia projektowanych systemów teleinformatycznych, bezpieczeństwa, aplikacji.

2.43 Wymagania i założenia podstawowe dla poszczególnych części sieci LAN i WLAN

W ramach zaprojektowanej sieci LAN i WLAN, przyjmuje się następujące wymagania ogólne, dotyczące zaproponowanych rozwiązań sieciowych:

- Systemy zarządzania/utrzymania/monitorowania aplikacji jak i kontroli dostępu do sieci, dla poszczególnych systemów, podłączane są w centralnym punkcie dostępu do sieci (serwerownia główna) – z uwzględnieniem wstępnie zakładanych wydajności i ilości jednocześnie zarządzanych urządzeń końcowych sieci LAN i WLAN. Wstępne założenia przedstawione są szczegółowo w dalszej części projektu.
- System kontroli dostępu do sieci LAN i WLAN, jest zunifikowany, oparty o jednolity system NAC (z odpowiednimi modułami funkcjonalnymi, opisanymi w dalszej części projektu), zintegrowany z pozostałymi systemami do kontroli/utrzymania/monitorowania sieci komputerowej. Minimalne wymagania na integrację poszczególnych systemów, zostały przedstawione w dalszej części projektu.
- Zaprojektowana sieć bezprzewodowa realizuje funkcje lokalizacji, na wyznaczonych piętrach, z zachowaniem standardów 802.11 ax. Zarządzanie poszczególnymi punktami dostępu do sieci bezprzewodowej odbywa się z poziomu kontrolera w postaci sprzętowej wirtualnej lub chmurowej.
- Zasilanie dla poszczególnych punktów dostępu do sieci bezprzewodowej odbywa się poprzez standard Power over Ethernet, z poziomem mocy wymagany per urządzenie, przy czym ze względu na zachowanie jednolitej platformy sprzętowej i programowej, zakłada się wykorzystanie przełączników ze standardem PoE+. Szczegółowa specyfikacja wymagań per wymagane urządzenie przedstawiona jest w dalszej części projektu.

2.44 Wymagania szczegółowe dla systemów zarządzania i monitorowania infrastrukturą sieciową i dostępem do sieci LAN i WLAN

W ramach projektu planuje się wdrożenie systemu zarządzania i monitorowania siecią teleinformatyczną. Zasadniczymi zadaniami systemu będą monitorowanie stanu infrastruktury, centralizacja procesów zarządzania i konfiguracji urządzeń sieciowych, kontrolowanie i uwierzytelnianie podłączających się do infrastruktury urządzeń końcowych. W ramach realizacji oczekuje się dostarczenia zestawu zintegrowanych wzajemnie narzędzi stanowiących jednolity system zarządzania infrastrukturą sieciową. Systemem zarządzania objęte zostaną wszystkie urządzenia przewodowej sieci dostępowej oraz urządzenia bezprzewodowej sieci WLAN.

System stanowić będzie centralny punkt zarządzania infrastrukturą sieciową poprzez

graficzny interfejs WWW. System zarządzania wykorzystywany będzie do konfiguracji urządzeń infrastruktury dostępowej, wdrażania w nich konfiguracji lokalnych sieci VLAN, śledzenia atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć. Wymaga się, aby system umożliwiał podgląd i modyfikacje parametrów wszystkich portów urządzeń sieciowych w zakresie konfiguracji przepustowości, sieci VLAN, metody autentykacji i parametrów protokołu Spanning Tree. System musi w sposób automatyczny wykrywać i lokalizować urządzenia podłączone do sieci, przechowywać ich atrybuty i raportować o ich stanie. System musi prowadzić zautomatyzowaną inwentaryzację urządzeń pracujących w sieci, w szczególności na zarządzanie spisem infrastruktury oraz dokumentacji i aktualizacji danych na temat zmian w infrastrukturze. System wykorzystywany będzie do administracji urządzeniami na poziomie plików konfiguracyjnych, planowania aktualizacji oprogramowania firmware, archiwizacji danych konfiguracyjnych, śledzenia wprowadzanych zmian w konfiguracji oraz przywracania konfiguracji.

System musi pozwalać na automatyczne generowanie reprezentacji wizualnej połączeń sieciowych tworząc mapy topologii sieci. Oczekuje się również, że rozwiązanie będzie umożliwiało graficzną lokalizację podłączonych urządzeń końcowych. W przypadku przewodowej sieci LAN musi być jednoznaczne wskazanie urządzenia i portu, do którego podłączone jest urządzenie wraz ze wskazaniem go na mapie. Lokalizacja urządzeń sieci bezprzewodowej WLAN musi jednoznacznie wskazać punkt dostępowy do którego podłączone jest aktualnie urządzenie oraz jego przybliżoną lokalizację w formie graficznej. System będzie centralnym punktem konfiguracji, wdrażania i egzekwowania polityk bezpieczeństwa zarówno dla przewodowej sieci LAN, jak i systemów podłączonych do bezprzewodowej sieci WLAN.

System posłużyć ma do aktywnego przyznawania dostępu do infrastruktury sieciowej określonym użytkownikom i urządzeniom końcowym w oparciu o informacje pochodzące z serwera usług katalogowych (np. Active Directory) poprzez przyznawanie określonego profilu bezpieczeństwa chroniąc tym samym infrastrukturę przed nieautoryzowanym dostępem do zasobów sieciowych. System kontroli dostępu musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci z wykorzystaniem protokołu IEEE 802.1X lub adresu MAC urządzenia.

System służyć będzie do uwierzytelniania:

- komputerów użytkowników,
- użytkowników (w przypadku współdzielonych urządzeń),
- drukarek sieciowych,
- telefonów IP, itp.

System musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i adresów IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych. Wymaga się, aby dostarczony system umożliwiał wyświetlenie w pojedynczym widoku następujących informacji na temat podłączonego systemu końcowego:

- przypisany adres IP,
- fizyczny adres MAC urządzenia,
- nazwa użytkownika (jeżeli występuje),
- adres IP przełącznika, do którego podłączone jest urządzenie końcowe
- port przełącznika, do którego podłączone jest urządzenie końcowe,

- metoda wykorzystana do uwierzytelniania systemu końcowego,
- stan autoryzacji systemu końcowego,
- czas pierwszego podłączenia się do sieci,
- czas ostatniego podłączenia się do sieci.

Powyższe informacje muszą być dostępne niezależnie czy urządzenie lub użytkownik podłączony jest do infrastruktury sieciowej za pośrednictwem przewodowej sieci LAN czy bezprzewodowej sieci WLAN.

Wymaga się również aby system umożliwiał wymianę informacji z wykorzystaniem interfejsu XML API z innymi systemami sieciowymi. W szczególności oczekuje się integracji systemu z zaporą sieciową firewall..

System musi umożliwiać rozbudowę w przyszłości o moduł analizy przepływów sieciowych w warstwach L2 do L7 w sieci wewnętrznej, ze szczególnym naciskiem na identyfikację sesji aplikacji sieciowych. Wdrożenie architektury opartej na przepływach sieciowych powinno umożliwiać w przyszłości monitorowanie i zbieranie danych statystycznych od warstwy L2 do L7 dla każdej pojedynczej zestawianej sesji ruchu sieciowego. Rozwiązanie musi posiadać zestaw sygnatur aplikacji do wykrywania wewnętrznie świadczonych aplikacji (Exchange, SQL, itp.), aplikacji działających w chmurze publicznej (Google, poczta elektroniczna, YouTube, P2P, współdzielenie plików, itp.), a także aplikacji społecznościowych (Facebook, Twitter, itp.) oraz wszelkich sesji RTP takich jak głos i wideo. Dodatkowo system musi w sposób ciągły monitorować usługi sieciowe uruchomione w sieci Zamawiającego takie jak: DHCP, DNS, NTP, LDAP itp.

System musi posiadać wbudowany moduł weryfikacji konfiguracji urządzeń sieciowych pod kątem wytycznych HIPAA, PCI oraz GDPR. Zmniejszy on ryzyko błędnej konfiguracji, nieprawidłowej klasyfikacji lub nieprzestrzegania norm branżowych. System powinien działać w oparciu o audyty i zdefiniowane przez użytkownika szablony zgodności. Mieć możliwość skonfigurowania harmonogramu dla automatycznej, systematycznej weryfikacji urządzeń sieciowych oraz generować raporty z tych czynności.

Warunkiem nadrzędnym jest, aby wszystkie wymienione powyżej funkcjonalności dostępne były za pośrednictwem pojedynczego interfejsu graficznego z poziomu przeglądarki WWW. W ramach zaprojektowanej infrastruktury, nie dopuszcza się dostarczenia rozwiązania spełniającego powyższe wymagania w formie odrębnych rozwiązań zarządzanych z osobna, w pełni nie zintegrowanych ze sobą.

System zarządzania i kontroli dostępu musi zostać objęty min. 3 letnim wsparciem serwisowym producenta. Musi ono obejmować wsparcie przez telefon/email/portał www w trybie 24/7, oraz umożliwiać aktualizacje systemu. Dodatkowo jeżeli w systemie są licencje czasowe na określone funkcjonalności to Zamawiający wymaga dostarczenia ich na okres minimum 3 lat.

2.45 Wymagania szczegółowe dla systemu zarządzania siecią LAN i WLAN

Funkcjonalność systemu zarządzania siecią i poszczególnymi urządzeniami

- Musi zapewniać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia.

- Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji.
- Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci.
- Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN.
- Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II.
- Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent.
- Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć.

Architektura

- Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami sieci przewodowej.
- Musi zawierać zintegrowane aplikacje typu plug-in, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania.
- Musi mieć możliwość instalacji, jako maszyna wirtualna.
- Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
- Rozwiązanie musi integrować się ze środowiskiem wirtualnym VMware ESX i ESXi.

Raportowanie

- Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci.
- Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (OID).
- Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).
- Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia.
- Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiegokolwiek zmiany w urządzeniu.
- Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu firmware urządzenia.
- Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń.
- Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych.
- Musi zapewniać możliwości analiz na poziomie portu.
- Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów.

Narzędzia administracyjne

- Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania.
- Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB (Management Information Base) z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB.
- Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby.
- Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania firmware i wielkość pliku konfiguracyjnego.
- Musi posiadać możliwość pobierania oprogramowania firmware do jednego urządzenia lub do wielu urządzeń jednocześnie.
- Musi mieć możliwość pobierania obrazów boot PROM do jednego urządzenia lub do wielu urządzeń jednocześnie.
- Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń.
- Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń.
- Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania.
- Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury.
- Musi umożliwiać automatyczną reakcję w czasie rzeczywistym poprzez integrację z rozwiązaniami klasy SIEM oraz IPS.
- Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym.

Bezpieczeństwo

- Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji.
- Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https.
- Musi mieć możliwość definiowania polityk:
 - ograniczających poziom pasma,
 - ograniczających liczbę nowych połączeń sieciowych,
 - ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3,
 - nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania
- Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą aplikacji, dzięki której polityki zostaną rozesłane do wszystkich urządzeń.
- Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci.
- Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC.

- Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p.

Kontrola

- Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia.
- Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzаныmi działaniami i nieuprawnionym zachowaniem sieci.
- Musi mieć możliwość przypisania „roli kwarantanny” użytkownikowi podłączonemu do portu.
- Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji.
- Musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci. Możliwość przypisywania sieci VLAN, reguł filtrowania warstw L2-L4 oraz QoS na warstwach L2-L4 (DSCP i 802.1p) dla każdej maszyny wirtualnej opartej na przełączniku wirtualnym i wirtualnej grupie portów. Reguły filtrowania na warstwach L3-L4 i reguły QoS muszą obsługiwać zarówno IPv4, jak i IPv6.

Skalowalność

System w początkowej fazie realizacji, objętej niniejszym projektem, musi obsługiwać wszystkie urządzenia sieciowych (10 przełączników i 18 punktów dostępowych) oraz umożliwiać w przyszłości rozbudowę do min. 50 urządzeń sieciowych.

2.46 Wymagania szczegółowe dla kompleksowego systemu kontroli dostępu do sieci

System kontroli dostępu do sieci LAN i WLAN, w pełni zintegrowany, zapewnia realizację zabezpieczeń na poziomie sieciowym, zwiększając poziom bezpieczeństwa i zapobiegania przed zagrożeniami, nieautoryzowanego dostępu do sieci, bądź dostępu do sieci niezgodnie z wymaganą polityką bezpieczeństwa. W tym w ramach systemu realizowany, zgodnie z późniejszą polityką bezpieczeństwa będzie dostęp gościnny, z zapewnieniem dostępu do wybranych zasobów sieciowych i systemów czy do sieci Internet. Obecnie, szczególnie w otwartych strukturach sieci, jest to bardzo istotny komponent sieciowy, zwiększający poziom bezpieczeństwa wykorzystywanych systemów.

Funkcjonalność

- System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem:
 - o standardu 802.1X
 - o adresu MAC urządzenia
 - o formularza webowego
- System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) 802.1X opartych o złożone i wielowarunkowe reguły profili bezpieczeństwa.
- System powinien aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów.

- System powinien współpracować z rozwiązaniem Microsoft NAP (Network Access Protection).
- Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych.
- Musi zapewniać możliwość powiadamiania poprzez Syslog oraz pocztę elektroniczną o sytuacjach krytycznych.
- System musi umożliwiać wysyłanie powiadomień mailowych z wykorzystaniem protokołu SMTP.
- System musi posiadać wewnętrzną bazę użytkowników. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych przy pomocy interfejsu programistycznego.
- Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania i autoryzacji podłączanych systemów końcowych.
- Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP.
- Rozwiązanie musi obsługiwać lokalną autoryzację MAC.

Profilowanie urządzeń

- System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, HTTP, RADIUS, Network Scan (NMAP), DNS, SNMP.
- System musi umożliwiać dodawanie rozpoznanych urządzeń do grupy.
- System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu. Musi istnieć możliwość przyznania określonego dostępu na podstawie informacji o urządzeniu dla co najmniej 1000 urządzeń.
- System musi rozpoznawać co najmniej następujące rodzaje urządzeń:
 - urządzenia z systemem Android,
 - Apple iPad, Apple iPhone, Apple iPod,
 - drukarki,
 - telefony IP,
 - stacja robocza z systemem Microsoft Windows,
 - stacja robocza z systemem MAC OS,
 - stacja robocza z systemem Linux.

Architektura

- System musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych i/lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości stopniowego zwiększania wydajności systemu – w momencie dostawy na co najmniej dwóch niezależnych serwerach,
- System musi być dostarczony w formie maszyny wirtualnej (wymagane wsparcie dla VMware ESXi i Hyper-V) obejmującej wszystkie elementy funkcjonalne kontroli dostępu, przy czym zamawiający dopuszcza rozwiązanie, gdzie zarządzanie i

monitorowanie systemu zostanie zainstalowane na dedykowanej do tego maszynie wirtualnej.

- W związku z istotnością systemu dla poprawnego funkcjonowania całej sieci system musi umożliwiać realizację wysokiej dostępności poszczególnych elementów funkcjonalnych typu 1:1 lub N+1.
- Musi zapewniać rozwiązanie NAC typu out-of-band, które może być zarządzane przez jedną centralną aplikację. Wszystkie urządzenia typu NAC Gateway powinny być zarządzane i monitorowane z jednej, centralnej konsoli.
- Musi być dostarczone jako maszyna wirtualna lub jako dedykowane rozwiązanie sprzętowe.
- System musi umożliwiać obsługę co najmniej 1000 urządzeń równocześnie podłączonych do sieci lokalnej LAN oraz sieci bezprzewodowej WLAN.
- Rozwiązanie powinno wspierać możliwość rozbudowy do min. 3000 sesji autoryzacyjnych bez potrzeby rozbudowy systemu o dodatkowe serwery fizyczne lub wirtualne - poprzez dodanie do systemu odpowiednich licencji.
- System musi umożliwiać rozbudowę w przyszłości o narzędzie do oceny stanu zabezpieczeń systemu końcowego – oczywiście w pełni zintegrowane z systemem i zarządzane poprzez ten sam interfejs WWW. Ocenianie musi być możliwe zarówno bez dedykowanego agenta instalowanego na stacji końcowej jak i z użyciem agenta. Ocenianie w oparciu o agenta dostępnego powinno być dostępne dla co najmniej komputerów z systemem Windows (2000, XP, Vista, 7, 8, 8.1, Server 2003, Server 2008) i MAC OS X musi umożliwiać następujące testy:
 - minimalna wersja agenta,
 - test wersji systemu operacyjnego,
 - test antywirusa (niezainstalowany/zainstalowany, uruchomiony, zaktualizowany, uruchomione RTP),
 - test zapory (uruchomiona/wyłączona) z możliwością automatycznego naprawienia niezgodności,
 - test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie),
 - test usługi Auto Update z opcją automatycznego naprawienia niezgodności,
 - test czasu od ostatniej aktualizacji systemu,
 - test wygaszacza ekranu (włączony, zabezpieczony hasłem, z określonym czasem aktywacji,
 - test obecności/niewystępowania pliku o określonej nazwie i sumie kontrolnej,
 - test wymagający braku występowania albo braku uruchomienia oprogramowania P2P z możliwością automatycznego naprawienia niezgodności,
 - test procesu (uruchomiony/nieuruchomiony) z opcją automatycznego naprawienia niezgodności,
 - test rejestru dla systemów Windows (obecność klucza/zbioru kluczy o konkretnej nazwie, typie wartości i wartości, równy bądź różny zadanemu),
 - test usługi (niezainstalowana/zainstalowana/uruchomiona),
 - test aplikacji (sprawdzenie obecności zainstalowanej aplikacji o konkretnej nazwie).

Narzędzie takowe dodatkowo powinno mieć możliwość dowolnego dobierania testów ww. rodzajów tworząc schematy oceniania, które będą aplikowane dla wszystkich grup urządzeń i użytkowników bądź dla wybranej grupy urządzeń i użytkowników. Podczas oceniania systemu końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów.

Musi być możliwość określenia oceniania jednorazowego przy wstępnym uwierzytelnianiu bądź oceniania wielokrotnego, o częstotliwości oceniania danej grupy urządzeń i użytkowników w zakresie od minut do tygodni. System końcowy podlegający kwarantannie musi otrzymać informację o testach zakończonych niepowodzeniem wraz ze wskazówkami ich poprawienia.

Zarządzanie systemem

- System musi posiadać graficzny interfejs zarządzania – zarządzanie poprzez przeglądarkę internetową lub dedykowaną aplikację.
- System musi umożliwiać uwierzytelnienie i autoryzację dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników oraz zewnętrzne repozytorium użytkowników.
- System musi umożliwiać definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania.
- System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych.

Zarządzanie dostępem gościnnym

- System musi umożliwiać realizację dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN przy pomocy portalu webowego. Formularz musi obsługiwać co najmniej następujące przeglądarki: Microsoft IE, Mozilla Firefox, Safari.
- Rozwiązanie musi posiadać funkcję portalu rejestracyjnego, aby zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
- Możliwość sponsorowania dostępu takie jak sponsorowanie email wraz z portalem dla sponsorów służący do zatwierdzania rejestracji gości.
- Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych o wybranej długości, mogących składać się z różnego rodzaju znaków.
- System musi umożliwiać rejestrację przez logowanie do Facebooka. Użytkownik po podaniu danych logowania do serwisu Facebook widzi informacje z publicznego profilu, jakie zostaną pobrane celem rejestracji w sieci.
- System musi umożliwiać dopasowanie wyglądu portalu wybranym użytkownikom i portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania i zmianę koloru tła.

2.47 Minimalne wymagania techniczne dla wewnętrznego punktu dostępowego sieci bezprzewodowej.

- Punkty dostępowe muszą być przeznaczone do pracy w środowisku o dużym zagęszczeniu urządzeń mobilnych (high density).
- Punkty dostępowe zasilane muszą być za pomocą standardu Power over Ethernet (PoE) IEEE 802.3af.

- Muszą obsługiwać równolegle dwa pasma częstotliwości 802.11ax/ac/a/n (5 GHz) i 802.11ax/n/b/g (2.4GHz).
- Punkty dostępowe muszą mieć możliwość rejestracji w centralnym systemie zarządzania.
Zamawiającego bez konieczności wykonywania konfiguracji na punkcie dostępowym niezależnie od miejsca podłączenia punktu dostępowego do sieci.
Funkcjonalność ta musi działać zarówno w przypadku podłączenia punktu dostępowego:
 - w podsięci zarządzania Zamawiającego (komunikacja L2 do systemu zarządzania).
 - w dowolnej innej podsięci sieci LAN Zamawiającego (komunikacja L3 do systemu zarządzania).
- Muszą posiadać możliwość konfiguracji przynajmniej jednego radia do pracy w paśmie 2.4GHz lub 5GHz. Muszą wspierać możliwość uruchomienia obydwu interfejsów radiowych w paśmie 5 GHz w celu zwiększenia przepustowości sieci, w przypadku gdy radio w paśmie 2.4 GHz będzie wyłączone ze względu na występujące interferencje.
- Muszą posiadać minimum 2 anteny wewnętrzne dookólne dla pasma 2.4GHz o mocy co najmniej 2,6dBi oraz 2 anteny wewnętrzne dookólne dla pasma 5GHz o mocy co najmniej 3,7dBi.
- Wsparcie dla standardu 802.11ax/ac co najmniej 2x2 MIMO.
- Min. 1 x Port 10/100/1000 Base-T RJ-45 z technologią autosensing.
- Obsługa min. 16 SSID na częstotliwość radiową.
- Zintegrowany Statefull Inspection Firewall.
- Zintegrowana funkcjonalność wykrywania i blokowania aplikacji (L7 firewall).
- Muszą posiadać chip TPM (Trusted Platform Module).
- Zintegrowany serwer Radius, dopuszczalne jest również zapewnienie funkcjonalności serwera Radius dowolnym innym elemencie dostarczanego systemu sieci WiFi.
- Przycisk resetu urządzenia do ustawień fabrycznych umożliwiający przywrócenie domyślnej
- konfiguracji fabrycznej w przypadku utraty połączenia do systemu zarządzania bez konieczności logowania się do systemu punktu dostępowego.
- Punkt dostępowy musi mieć możliwość montażu na suficie.
- Wymagane obsługiwane standardy sieciowe min. :
 - IEEE 802.11a,
 - IEEE 802.11b,
 - IEEE 802.11e,
 - IEEE 802.11g,
 - IEEE 802.11i,
 - szyfrowanie AES/CCMP i TKIP,
 - IEEE 802.11n,
 - IEEE 802.11ac,
 - IEEE 802.11ax,
 - IEEE 802.3af,

- IEEE 802.1x,
- Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2) oraz Wi-Fi Protected Access 3 (WPA3),
- wsparcie dla kanałów radiowych o szerokości 20MHz, 40MHz i 80MHz,
- zgodność z DFS2 (Dynamic Frequency Selection),
- punkt dostępowy musi obsługiwać funkcję IP QoS w środowisku przewodowym i bezprzewodowym (802.1p, diffserv i policing).

2.48 Minimalne wymagania techniczne dla przełącznika rdzeniowego sieci LAN

- Wysokość urządzenia 1U
- Przełącznik posiadający minimum 24 porty 10GBase-X (SFP+)
- Przełącznik posiadający minimum 2 porty QSFP28
- Przełącznik posiadający miejsce na dodatkowy moduł mogący, w zależności od potrzeb, być obsadzonym:
 - 4 portami 1/10GBase-X (SFP+)
 - 4 portami 10/25GBase-X (SFP28)
- Nieblokującą architekturę o wydajności przełączania min. 1080 Gb/s
- Szybkość przełączania min. 800 Milionów pakietów na sekundę
- Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management
- Wbudowany port USB oraz port konsoli
- Przełącznik musi posiadać wbudowane, redundantne zasilacze 230V AC
- Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
- Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
- Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
- Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. System musi mieć możliwość dodania nowego modułu lub aktualizacji już zaimplementowanych bez konieczności restartu całego urządzenia
- Możliwość monitorowania zajętości CPU
- Routing statyczny
- Obsługa routingu dynamicznego IPv4
 - RIPv1/v2, OSPFv2
 - BGP, IS-IS – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
- Policy Based Routing dla IPv4
- Obsługa routingu dynamicznego dla IPv6
 - RIPv6, OSPFv3
 - BGP, IS-IS – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
- Policy Based Routing dla IPv6
- Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
- Obsługa IGMP v1/v2/v3 oraz IGMP v1/v2/v3 snooping
- Obsługa protokołu PIM-SM

- Obsługa Network Login
 - IEEE 802.1x
 - Web-based Network Login
 - MAC based Network Login
- Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
- Obsługa wielu klientów (min. 12) Network Login na jednym porcie (Multiple supplicants)
- Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
- Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
- Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągle zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma
- Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
 - definicji sieci VLAN,
 - reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
 - realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
 - realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
- Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication
- Bezpieczeństwo MAC adresów:
 - ograniczenie liczby MAC adresów na porcie
 - zatrzaśnięcie MAC adresu na porcie
 - możliwość wpisania statycznych MAC adresów na port/vlan
 - możliwość wyłączenia MAC learning
- Zabezpieczenie przełącznika przed atakami DoS
 - Networks Ingress Filtering RFC 2267
 - SYN Attack Protection
 - Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
- Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika – wire-speed)
- Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
- Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
- Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768)
- Obsługa STP, RSTP, MSTP, PVST+
- Obsługa protokołu MVRP
- Obsługa EAPS (RFC 3619)
- Obsługa protokołu ERPS lub równoważnego oraz ITU G.8032
- Obsługa Link Aggregation IEEE 802.3ad wraz z LACP
- Obsługa IEEE 802.3ah Ethernet OAM

- Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników
- Musi mieć możliwość zarządzania za pomocą SSH/Telnet, SNMP, oraz systemu zarządzania dostarczonego przez producenta
- Zarządzanie przez SNMP v1/v2/v3
- Obsługa SYSLOG z możliwością definiowania wielu serwerów
- Sprzętowa obsługa sFlow lub protokołu równoważnego
- Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
- Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
- Możliwość uruchamiania skryptów:
 - Ręcznie
 - O określonym czasie lub co wskazany okres czasu
 - Na podstawie wpisów w logu systemowym
- Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS
- Obsługa Data Center Bridging
 - Data Center Bridging Exchange Protocol (DCBx)
 - Priority Flow Control (PFC)
- Obsługa protokołu MACSEC (IEEE 802.1AE) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania
- Dożywotnia gwarancja producenta uwzględniająca:
 - wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego,
 - aktualizacje oprogramowania układowego (firmware),
 - wsparcie techniczne producenta przez serwis www,
 - dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.

2.49 Minimalne wymagania techniczne dla przełączników dostępowych sieci LAN.

Wymagania ogólne dla urządzeń typu Przełącznik dostępowy

- Wysokość urządzenia 1U
- Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T
- Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management
- Wbudowany port USB oraz port konsoli
- Przełącznik musi posiadać wbudowany zasilacz 230V AC, oraz musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza
- Możliwość łączenia do 8 przełączników w stos. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR/LR oraz włókien światłowodowych
- Tablica MAC adresów min. 16k
- Pamięć operacyjna: min. 1GB pamięci DRAM

- Pamięć flash: min. 4GB pamięci Flash oraz bufora pakietów min. 1,5MB
- Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
- Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
- Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
- Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. System musi mieć możliwość dodania nowego modułu lub aktualizacji już zaimplementowanych bez konieczności restartu całego urządzenia
- Możliwość monitorowania zajętości CPU
- Pojemność tabeli routingu IPv4 min. 480 wpisów
- Routing statyczny
- Obsługa routingu dynamicznego IPv4
 - RIPv1/v2
 - OSPFv2 – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
- Policy Based Routing dla IPv4
- Pojemność tabeli routingu IPv6 min. 240 wpisów
- Routing statyczny
- Obsługa routingu dynamicznego dla IPv6
 - RIPv6
 - OSPFv3 – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
- Policy Based Routing dla IPv6
- Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
- Obsługa IGMP v1/v2/v3 oraz IGMP v1/v2/v3 snooping
- Obsługa protokołu PIM-SM – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
- Obsługa Network Login
 - IEEE 802.1x
 - Web-based Network Login
 - MAC based Network Login
- Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
- Obsługa wielu klientów (min. 12) Network Login na jednym porcie (Multiple supplicants)
- Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
- Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
- Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma
- Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
 - definicji sieci VLAN,

- reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
 - realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
 - realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
- Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication
- Bezpieczeństwo MAC adresów:
 - ograniczenie liczby MAC adresów na porcie
 - zatrzaśnięcie MAC adresu na porcie
 - możliwość wpisania statycznych MAC adresów na port/vlan
 - możliwość wyłączenia MAC learning
- Zabezpieczenie przełącznika przed atakami DoS
 - Networks Ingress Filtering RFC 2267
 - SYN Attack Protection
 - Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
- Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika – wire-speed)
- Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
- Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
- Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768) – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
- Obsługa STP, RSTP, MSTP, PVST+
- Obsługa protokołu MVRP
- Obsługa EAPS (RFC 3619)
- Obsługa protokołu ERPS lub równoważnego oraz ITU G.8032
- Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – minimum 128 grup po 8 portów
- Obsługa IEEE 802.3ah Ethernet OAM
- Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników
- Musi mieć możliwość zarządzania za pomocą SSH/Telnet, SNMP, dedykowanego interfejsu przeglądarkowego, oraz systemu zarządzania dostarczonego przez producenta (zarówno wersji on-site jak i interfejsu chmurowego)
- Obsługa protokołu Zero Touch Provisioning (ZTP), pozwalającego na automatyczną konfigurację urządzeń z centralnego punktu zarządzania
- Zarządzanie przez SNMP v1/v2/v3
- Obsługa SYSLOG z możliwością definiowania wielu serwerów
- Sprzętowa obsługa sFlow lub protokołu równoważnego
- Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
- Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
- Możliwość uruchamiania skryptów:
 - Ręcznie
 - O określonym czasie lub co wskazany okres czasu
 - Na podstawie wpisów w logu systemowym
- Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS

- Obsługa protokołu MACSEC (IEEE 802.1AE) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania
- Wsparcie dla protokołów przeznaczonych do przesyłania w czasie rzeczywistym sygnałów audio, wideo oraz innych przez sieć Ethernet (np. RAVENNA, AVB lub równoważne) – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
- Dożywotnia gwarancja producenta uwzględniająca:
 - wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego,
 - aktualizacje oprogramowania układowego (firmware),
 - wsparcie techniczne producenta przez e-mail i serwis www oraz telefonicznie w dni robocze w godzinach 8-17,
 - dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.

2.50 Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 48 portowy POE+

Wszystkie zapisy ogólne dotyczące urządzeń typu Przełącznik dostępowy i dodatkowo:

- Przełącznik posiadający minimum 48 portów 1G 100/1000BASE-T POE+
- Przełącznik posiadający minimum 8 portów 1G SFP (mogą być porty typu Combo)
- Przełącznik mający możliwość rozbudowy (licencje – np. kosztem portów SFP, dodatkowy moduł) o 4 porty 10G SFP+.
- Nieblokującą architekturę o wydajności przełączania min. 176 Gb/s
- Szybkość przełączania min. 130 Milionów pakietów na sekundę
- W chwili dostawy musi gwarantować dostarczenie 740W mocy POE oraz standaryzację negocjacji zasilania za pomocą LLDP/LLDP-MED.
- Dodatkowo musi mieć możliwość, poprzez instalację dodatkowego zasilacza dostarczenie 30W mocy równocześnie na wszystkich 48 portach (1440W POE per przełącznik).

2.51 Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 24 portowy POE+

Wszystkie zapisy ogólne dotyczące urządzeń typu Przełącznik dostępowy i dodatkowo:

- Przełącznik posiadający 24 portów 1G 100/1000BASE-T
- Przełącznik posiadający 8 portów 1G SFP (mogą być porty typu Combo)
- Przełącznik mający możliwość rozbudowy (licencje – np. kosztem portów SFP, dodatkowy moduł) o 4 porty 10G SFP+.
- Nieblokującą architekturę o wydajności przełączania min. 128 Gb/s
- Szybkość przełączania min. 95 Milionów pakietów na sekundę
- W chwili dostawy musi gwarantować dostarczenie 380W mocy POE oraz standaryzację negocjacji zasilania za pomocą LLDP/LLDP-MED.

2.52 Wsparcie serwisowe

Wymagane jest, aby wszystkie urządzenia i systemy w niniejszym zamówieniu pochodziły od jednego producenta dla zapewnienia najwyższego możliwego stopnia współpracy urządzeń LAN, systemów zarządzania siecią i kontroli dostępu do sieci.

System wymaga dodatkowo zastosowania serwera; na serwerze zawarta będzie wirtualna maszyna bramy NAC.

Do wszystkich urządzeń i systemów powinna być dołączona 3-letni kontrakt serwisowy producenta obejmujący:

- wsparcie świadczone bezpośrednio przez producenta 24/7/365;
- wymiana uszkodzonego sprzętu NBD;
- zgłoszenia problemów przez telefon, email, portal www producenta;
- nielimitowana ilość zgłoszeń;
- dostęp do aktualizacji firmware oraz rozszerzeń;
- dostęp do najnowszych poprawek i dodatków Service Pack;
- pełny dostęp do bazy wiedzy pomocy technicznej producenta oraz forów produktów;

2.53 System telefonii VoIP

Minimalne wymagania dla systemu telefonii VoIP

- wewnętrzne telefony IP – 25,
- linii miejskich VoIP – 25,
- z telefonami systemowymi dedykowanymi przez producenta systemu – 25,
- niezbędne licencje: – 1,
- abonentów – 25,
- linkowanie licencja serwerowa NCP.Base100.Networking – 1,

Przewiduje się podłączenie nowo projektowanej centrali sieci telekomunikacyjnej Starostwa z budynkiem głównym.

2. INSTALACJA MONITORINGU

3.1 GENERALNE WYMAGANIA

Wszystkie urządzenia muszą być fabrycznie nowe i wyprodukowane nie wcześniej niż 9 miesięcy przed datą dostarczenia. W momencie oferowania wszystkie elementy oferowanego systemu muszą być dostępne (dostarczane przez producenta) w dacie złożenia oferty i nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży. Wszystkie komponenty danego urządzenia muszą pochodzić od jednego producenta

3.2 SYSTEM VMS

- Oprogramowanie musi posiadać czytelną, prostą politykę licencjonowania opartą o klucze licencyjne z możliwością ich grupowania w celu optymalizacji kosztowej dla użytkowników końcowych;
- Oprogramowanie musi opierać się o licencjonowanie dostępu (możliwości

- podłączenia) kamer wideo lub innych źródeł wideo o specyfice szczegółowo opisanej w dalszej części wymagań;
- Oprogramowanie musi być skalowalne od jednego klienta, serwera i kamery do setek klientów, serwerów i kamer;
 - Oprogramowanie musi posiadać elastyczną, skalowalną - co najmniej 3 stopniową skalę (wersję) funkcjonalności oprogramowania z możliwości migracji do wyższej wersji z niższej (mniejszej liczby funkcjonalności).;
 - Oprogramowanie musi udostępniać nieodpłatną aplikację kliencką bez ograniczeń ilościowych w instalacji w zakresie urządzeń – stacji oglądowych.
 - Oprogramowanie musi udostępniać pakiet SDK w celu integracji z rozwiązaniami trzecimi
 - Oprogramowanie musi udostępniać nieodpłatną wersję oprogramowania dla aplikacji mobilnych z obsługą urządzeń opartych, co najmniej o system iOS i Android
 - Oprogramowanie musi posiadać możliwość dostępu (na takich samych zasadach i w oparciu o te same funkcjonalności, co standardowa aplikacja kliencka oprogramowania) do systemu poprzez aplikację kliencką opartą o przeglądarkę internetową.
 - Rozbudowa systemu musi być możliwa w każdej chwili nawet o pojedynczą kamerę (licencję)
 - Aplikacja serwerowa nie może być ograniczona pod kątem producenta sprzętu, na którym ma pracować, a jedynie parametrami technicznymi i wydajnościowymi umożliwiającymi jej poprawne, płynne i nieprzerwane wykorzystanie;
 - Oprogramowanie zarządzające serwerem i klientem muszą posiadać możliwość instalacji na jednej maszynie jak również na oddzielnych tworząc architekturę klient-serwer;
 - praca w architekturze klient-serwer, w tym wiele serwerów i jeden klient oraz wiele serwerów i wiele stacji klienckich, a w ramach jednego systemu do najmniej 20 00 kamer i co najmniej 100 serwerów, wymaga się aby jednym logowaniem autoryzować się do wszystkich serwerów w systemie;
 - Otwarta architektura klient-serwer pozwalająca na podłączenie do systemu nielimitowanej liczby nowych urządzeń;
 - możliwość grupowania serwerów w ramach jednej „logicznej” lokalizacji, jako jeden system lub podsystem
 - możliwość nagrywania, z co najmniej 100 kamer na jednym serwerze
 - Wsparcie dla kamer sieciowych obsługujących powszechnie stosowane kompresje MJPEG, MPEG4, H.264, H.265;
 - obsługa kamer wysokich rozdzielczości (kamer megapikselowych) do 30 Mpix włącznie;
 - obsługa kamer producentów trzecich w oparciu o standard ONVIF oraz ewentualne natywne integracje;
 - obsługa kamer multisensorycznych – wieloprzetwornikowych;
 - Szybkość nagrywania: do 60 klatek na sekundę (na kamerę);
 - Oprogramowanie ma zapewnić grupowanie wszystkich serwerów w celu zapewnienia ciągłości pracy systemu na wypadek awarii któregoś z nich – dane o użytkownikach, ich aktywności zdarzeniach, alarmach pozostają niezmienione, nie ulegają utracie w sytuacji awarii któregoś serwera w sieci – grupie;
 - ustawienia rejestracji z indywidualnie (dla każdej rejestrowanej kamery) dobranymi

- parametrami zapisu;
- ustawienia parametrów rejestracji: ilość klatek/s, rozdzielczość, jakość kompresji przynajmniej 10 poziomów kompresji;
 - Oprogramowanie musi zapewnić opcję nagrywania „buforowego” przed zdarzeniem i nagrywania po zdarzeniu;
 - oprogramowanie musi zapewnić możliwość planowania kopii zapasowych z nagraniami wideo i zdarzeń do folderu lokalnego lub na zmapowany dysk sieciowy;
 - oprogramowanie musi posiadać możliwość automatycznego kasowania najstarszych kopii zapasowych w przypadku wyczerpania się miejsca do zapisu nowych kopii zapasowych.
 - oprogramowanie musi posiadać możliwość rejestracji strumieni audio i wideo w oparciu o harmonogram nagrywania, który można określić indywidualnie dla każdego źródła video. Harmonogram powinien zawierać obsługę następujących parametrów: tryb nagrywania, ciągle nagrywanie, nagrywanie na ruch, wejścia cyfrowe, alarmy, transakcje POS, tablice rejestracyjne, ustawienia daty i godziny, codziennie, tygodniowo;
 - oprogramowanie musi umożliwiać rejestrację w oparciu o nagrywanie ciągle, nagrywanie z detekcją ruchu lub zdarzenia;
 - możliwość zaimplementowania narzędzi (algorytmów) inteligentnej analizy obrazu (np. rozpoznawania tablic rejestracyjnych, analiza ruchu osób i pojazdów);
 - Oprogramowanie musi umożliwiać nagrywanie pierwszego lub drugiego lub trzeciego strumienia wideo z danego źródła wideo;
 - Oprogramowanie musi umożliwiać wysyłanie do aplikacji klienckiej dynamicznej zmiany strumienia w sytuacji wyświetlania obrazu wideo w podziale większym niż 1x1 w celu optymalizacji pasma transmisji pomiędzy aplikacją serwerową i kliencką;
 - Oprogramowanie musi być dostępne w następujących językach: polski, angielski, francuski, niemiecki, włoski, hiszpański, portugalski (Brazylia), portugalski (Portugalia), szwedzki, fiński, rosyjski, chiński (uproszczony), chiński (tradycyjny), japoński, koreański, arabski, hebrajski, japoński, turecki, duński, holenderski, czeski;
 - System nie może mieć ograniczeń pojemności zapisu i musi pozwalać na rozbudowę pojemności zapisu, do co najmniej 2000 TB;
 - Oprogramowanie musi umożliwiać aktualizację do najnowszej wersji bez konieczności odinstalowywania poprzedniej wersji;
 - oprogramowanie musi automatycznie wykrywać wszystkie serwery uruchomione na komputerach podłączonych do tej samej sieci co klient;
 - oprogramowanie musi mieć funkcję wyszukiwania, aby wykryć serwery uruchomione na komputerach połączonych w innym segmencie sieci niż klient, za pomocą adresów IP lub nazw hostów;
 - jednoczesna archiwizacja obrazu i jego odtwarzanie na wielu stanowiskach oglądowych w tym samym czasie;
 - oprogramowanie musi zapewnić możliwość ustawienia limitu maksymalnego pasma dla danych przesyłanych z aplikacji serwerowej do aplikacji klienckiej;
 - możliwość aktualizacji jednocześnie wszystkich serwerów pracujących w danej sieci z poziomu stacji klienckiej o odpowiednich uprawnieniach operatorskich;
 - oprogramowanie musi zawierać aplikację typu gateway, która pozwala podłączyć urządzenia mobilne do systemu.
 - Mobilny klient musi być obsługiwany przez urządzenia mobilne z systemem Android

- i Apple. Klient mobilny musi pozwalać na dostęp do wszystkich kamer w systemie z możliwością tworzenia widoków min. 4x4.
- oprogramowanie w wersji na urządzenia mobilne musi wspierać (obsługiwać) powiadomienia typu „push” generowane przez system i analizę wideo;
 - oprogramowanie musi zapewnić możliwość automatycznego logowania się do NVR (Serwera);
 - oprogramowanie musi zapewnić możliwość automatycznego wylogowania z NVR (Serwera), gdy aplikacja nie jest używana;
 - możliwość kooperacyjnej pracy operatorów systemu poprzez błyskawiczne dzielenie się oglądanymi obrazami przez jednego z nich np. w przypadku wystąpienia zdarzenia, kilku operatorów ma mieć możliwość oglądania dokładnie tego samego co wybrany operator;
 - system ma mieć możliwość rozbudowy o opcjonalny, w pełni integralny moduł rozpoznawania tablic rejestracyjnych (LPR);
 - możliwość przekazania informacji z tego samego alarmu wielu operatorom systemu wraz z ewentualną eskalacją zdarzeń;
 - oprogramowanie ma zapewniać kolaboracyjną współpracę niezależnych operatorów systemu poprzez możliwość przekazania przez jednego operatora oglądanych przez niego widoków z kamer innemu operatorowi w czasie rzeczywistym w celu szybszej analizy tych samych kluczowych zdarzeń z kamer przez kilku operatorów;
 - VMS musi posiadać dedykowaną aplikację do automatycznego (według ustalonego harmonogramu) zarządzania szczegółowymi ustawieniami wybranych kamer, takimi jak np. balans bieli, czas otwarcia migawki, maksymalny strumień, interwał klatek kluczowych i umożliwiający automatyczny restart kamer. Musi istnieć możliwości wymuszenia zmiany tych parametrów na podstawie określonych zdarzeń, takich jak np. sygnał ze zintegrowanego systemu zewnętrznego lub alarm z systemu analityki wideo;
 - VMS musi posiadać dedykowaną aplikację do automatycznego (według ustalonego harmonogramu) pobierania logów bezpośrednio z wybranych kamer;
 - VMS musi posiadać dedykowaną aplikację umożliwiającą automatyczne wykonywanie cyklicznych zrzutów obrazu (snapshotów) bezpośrednio z kamer i ich transmisję do ustalonej lokalizacji (np. centrali) w przypadku utraty połączenia pomiędzy kamerą i serwerem VMS. Dodatkowo musi istnieć możliwość efektywnego zarządzania zgromadzonymi zrzutami (wyszukiwanie, przeglądanie, archiwizacja).
 - VMS musi posiadać funkcję automatycznej aktualizacji firmware kamer oraz możliwość ładowania firmware do kamer z pliku.
 - system musi posiadać funkcjonalność umożliwiającą rejestrację jednocześnie strumienia danych niskiej i wysokiej jakości. Administrator musi mieć możliwość zdefiniowania okresu przechowywania strumienia wysokiej jakości, tak, aby strumień ten został usunięty po określonym czasie a strumień niskiej jakości pozostawał do końca żądanego okresu przechowywania.;
 - system musi posiadać funkcjonalność umożliwiającą automatyczne zmniejszenie poklatkowości do 1/2 lub 1/4 eksportu materiału wizyjnego w celu optymalizacji czasu zgrywanego materiału;
 - oprogramowanie do zarządzania wideo w sieci (musi umożliwiać zarządzanie i synchronizację serwerów w obszarze (site) z dzielonymi i rozproszonymi danymi i

ustawieniami systemu, tak, aby awaria dowolnego serwera nie powodowała utraty danych i ustawień systemu;

- oprogramowanie musi posiadać możliwość przesyłania tylko wybranych fragmentów obrazu pomiędzy serwerami rejestrującymi a stacjami operatorskimi w celu optymalizacji dostępnego pasma z zastrzeżeniem rejestracji na serwerach zapisu obrazów z najlepszą dostępną jakością;
- oprogramowanie musi posiadać możliwość automatycznej aktualizacji całego systemu, czyli wszystkich serwerów i stacji klienckich do najnowszej dostępnej wersji;

3.3 APLIKACJA KLIENCKA

- Panel główny aplikacji klienckiej musi być w pełni konfigurowalny w zakresie, co najmniej: wyświetlanych źródeł wideo, map, zdarzeń alarmowych, zapisanych widoków;
- Panel Główny musi posiadać czytelne i przejrzyste drzewo katalogowe pozwalające na pełną jego konfigurację w zakresie typów wyświetlanych urządzeń, serwerów, widoków, lokalizacji;
- Panel główny aplikacji klienckiej musi umożliwiać dostęp za pomocą pojedynczego kliknięcia do materiału wideo w trybie „na żywo” i „nagranego”;
- Panel główny musi umożliwiać wyszukiwanie pojedynczych zasobów, do których danych użytkownik ma dostęp, co najmniej takich jak: dany serwer, dana mapa, dana kamera, dany widok wideo, dany adres www;
- Panel główny musi posiadać, co najmniej poniższe przyciski do obsługi wideo:
 - a) kursor myszy do wyboru danego serwera, danej kamery, mapy, danego widoku wideo, danego adresu www czy innej akcji jaką użytkownik chce wywołać;
 - b) Przyciski zoomu cyfrowego „in plus” i „in minus”
 - c) przycisk do pracy na przybliżonym materiale wideo
 - d) przyciski do sterowania PTZ
 - e) Przycisk do wyboru układu wyświetlania obrazów wideo i innych źródeł danych
 - f) przycisk maksymalizacji danego źródła danych lecz nie mniej niż obrazu z kamery i mapy
 - g) przycisk przełączania pomiędzy widokami z kamer
 - h) przycisk zapisu danego widoku z kamer
 - i) przycisk przesłania danego widoku do innego operatora – funkcja współpracy operatorów
- Dostęp do widok z danego zasobu z panelu wideo musi odbywać się zarówno poprzez dwukrotny klik lewego przycisku myszki jak i poprzez funkcję „przenieś i upuść”;
- Panel Główny musi posiadać narzędzie do wyświetlania kluczowych informacji dla użytkownika wraz, z co najmniej 2 kolorową skalowalnością istotności informacji.
- Panel Główny aplikacji musi posiadać możliwość minimalizacji okna, maksymalizacji i zamknięcia aplikacji klienckiej
- Panel Główny aplikacji musi umożliwiać pracę opartą o zakładki zawierające widoki z wybranych przez użytkownika kamer czy innych źródeł informacji, przy czym użytkownik musi posiadać pełnię możliwości kreowania informacji w każdej zakładce w ramach posiadanych uprawnień;

- Panel Główny musi umożliwiać otwarcie co najmniej 20 różnych zakładek zawierających co najmniej wszystkie poniższe dane:
 - a) Widok (Logowanie do danej lokalizacji, nowy widok, alarmy i zarządzanie nimi)
 - b) Wyszukiwanie zdarzeń (Zdarzenia takie jak: ruch, wejście cyfrowe, obiekty sklasyfikowane, miniatury, zdarzenia alarmowe, transakcje POS, zakładki „bookmark”
 - c) Eksport (Eksport materiału i archiwizacja)
 - d) Zarządzanie (Konfiguracja witryny, dziennik witryny)
- Panel Główny musi posiadać przycisk do konfiguracji aplikacji klienckiej;
- Panel Główny musi posiadać w trybie oglądu materiału nagranych oś czasu z wyświetlaniem co najmniej poniższych informacji: materiał nagrany ciągle, materiał z występowaniem ruchu, dokładna data materiału wideo, informacja o oglądanej kamerze i kamerach (jednocześnie ogląd),
- Panel Główny musi mieć możliwość odtwarzania materiału wideo w trybie prędkości od -8X do +8X wraz z prędkościami cząstkowymi -1/4, -1/2, 1/2, 1/4 ;
- oprogramowanie musi umożliwiać tworzenie zakładki na nagranych wideo i audio z wielu źródeł, wyświetlanie zakładki na osi czasu, i opcję wyszukiwania zakładki;
- oprogramowanie musi umożliwiać ochronę zakładki tak, aby dane wideo i audio nie były nadpisywane;
- oprogramowanie musi umożliwiać przeszukiwanie zakładki na podstawie różnych kryteriów, w tym nazwy zakładki, notatek i powiązanych nazw kamer;
- możliwość tworzenia, edycji, usuwania zakładki „bookmark” dla operatorów (klientów) pracujących w oparciu o klienta sieciowego HTML;
- Panel Główny musi posiadać możliwość automatycznego, cyklicznego przełączania pomiędzy otwartymi zakładkami wideo;
- Przycisk do konfiguracji Panelu Głównego musi umożliwiać dostęp, do co najmniej: konfiguracji aplikacji klienckiej, instrukcji obsługi, otwarcia nowego okna, zalogowanie się, wylogowanie się, wygenerowanie raportu błędów;
- W ramach konfiguracji aplikacji klienckiej muszą być dostępne, co najmniej poniższe funkcje: wyświetlania powiadomień, synchronizacja odtwarzanego materiału wideo, wybór języka aplikacji klienckiej, automatyczne logowanie do witryny z opcją uwierzytelniania Windows oraz poprzez wpisanie loginu i hasła, zdefiniowanie pasma pomiędzy klientem i serwerem;
- W ramach konfiguracji aplikacji klienckiej musi istnieć możliwość tworzenia nakładek obrazu takich jak: nazwa kamery, lokalizacja kamery, sygnatura czasowa, datownik „na żywo”, wskaźnik nagrywania, aktywność ruchu (miejsce występowania ruchu), zdarzenia analizy obrazu, tablice rejestracyjne, jakość wyświetlania obrazu w aplikacji klienckiej – co najmniej 3 różne poziomy
- Panel Główny musi umożliwiać oglądanie pełnych jakościowo obrazów, wsparcie dla kompresji, co najmniej: MJPEG, MPEG4, H.264, H.265
- Panel Główny musi umożliwiać tworzenie zakładki wraz panelami wideo do oglądu obrazów z kamer w trybie „na żywo” jak i nagranych materiału wideo;
- W ramach jednej zakładki wideo system musi umożliwiać wyświetlanie do 64 obrazów (paneli wideo) z kamer w podziale 8x8;
- Oprogramowanie musi zapewniać możliwość wyświetlania na tym samym monitorze podpiętym do tej samej stacji klienckiej obrazu z wybranej kamery w trybie „na żywo” i „nagranych”;
- Aplikacja musi umożliwiać pracę na stanowisku wielomonitorowym, – co najmniej 4

monitorów podłączonych bezpośrednio do stacji roboczej oraz monitów wyniesionych podłączonych przez sieć IP z możliwością zarządzania z jednego PC.

- W ramach pracy wielomonitorowej aplikacja kliencka musi posiadać możliwość wyświetlania jej na każdym monitorze niezależnie w ramach nowo otwartych okien;
- Każde nowo otwarte okno musi tworzyć nowy Panel Główny z wszystkimi funkcjonalnościami opisanymi, jako wymagania Panelu Głównego;
- W ramach wyświetlanych obrazów z kamer system musi umożliwiać wykonanie natychmiastowego zdjęcia w zadanej przez operatora jakości i rozdzielczości wraz z opcją wyboru formatu i obszaru eksportu z danego kadru;
- W ramach zapisu zdjęcia system musi umożliwiać korektę ustawień gammy, poziomu czerni i bieli
- Okno panelu wideo musi umożliwiać maksymalizację oglądu z danego źródła wideo jak i powrót do poprzedniej wielkości (przed wywołaniem trybu pełnoekranowego);
- W ramach panelu wideo system musi umożliwiać zapis wideo w trybie manualnym;
- W ramach panelu wideo użytkownik będzie posiadał możliwość zamknięcia danego widoku z kamery (panelu wideo);
- System musi umożliwiać zapis danego widoku wykorzystywanego przez użytkownika w celu późniejszego ponownego wykorzystania;
- W sytuacji wyświetlania kamery PTZ system będzie umożliwiał jej sterowanie w zakresie obrotu w pionie i poziomie, zoomu optycznego oraz cyfrowego;
- System musi umożliwiać w danym panelu wideo natychmiastowy dostęp na żądanie do materiału nagranego z ostatnich 30, 60, 90 sekund;
- System musi posiadać funkcję cyfrowego zoomu w podglądzie na żywo oraz przy odtwarzaniu nagrań z archiwum;
- oprogramowanie musi umożliwiać oglądanie tego samego strumienia wideo na żywo lub nagranego na różnych poziomach zoomu cyfrowego i na różnych obszarach widoku;
- oprogramowanie musi umożliwiać nawigację na nagraniach wideo i audio poprzez kalendarz, linię czasu lub zdarzenia;
- System musi umożliwiać transmisję dźwięku w danym panelu wideo: od wideo serwera do oprogramowania klienckiego, obsługa dźwięku w podglądzie na żywo oraz w podglądzie przy odtwarzaniu nagrań z archiwum;
- Oprogramowanie klienckie musi posiadać możliwość wyszukiwania

3.4 Ustawianie parametrów pracy kamer [Dla kamer stacjonarnych 1,2,3,5,8 16 i 30 megapikseli]

Oprogramowanie klienckie musi posiadać poniższe funkcjonalności związane z konfiguracją i parametryzacją pracy kamer. Wszystkie funkcjonalności muszą być dostępne z poziomu uprawnień administratora, jak również z poziomu uprawnień operatora o ile ma uprawnienia do zmiany części z nich.

- Oprogramowanie musi umożliwiać zamianę podstawowych parametrów kamery takich jak: nazwa kamery, lokalizacja kamery, logiczne ID;
- Oprogramowanie musi umożliwiać włączenie lub wyłączenie stanu diod LED kamery oraz działania analizy wideo o ile kamera podłączona do systemu jest w nią wyposażona;
- Oprogramowanie musi umożliwiać włączenie funkcji PTZ w sytuacji wykorzystania

RS485 w kamerze (o ile kamera ma takie złącze). W ramach funkcji PTZ musi istnieć możliwość wyboru protokołu transmisji, szybkości transmisji oraz parzystości;

- Oprogramowanie musi posiadać możliwość resetu kamery – ponownego uruchomienia;
- Oprogramowanie musi posiadać możliwość automatycznego i ręcznego nadania adresu IP;
- Oprogramowanie musi umożliwiać włączenie multiemisji wraz z możliwością ustawienia TTL;
- Oprogramowanie musi umożliwiać włączenie i zmianę:
 - e) trybu dziennego i nocnego kamery oraz automatycznego wyboru pracy trybu dzień/noc
 - f) zmianę ekspozycji ręczną i automatyczną
 - g) przesłony – otwartą, zamkniętą, automatyczną
 - h) maksymalny czas naświetlania
 - i) maksymalne wzmocnienie
 - j) BLC – Kompensacja tylnego światła
 - k) Nasycenie i wyostrenie
 - l) Obrót obrazu z kamery o 90°, 180°, 270°;
 - m) Automatyczny i niestandardowy balans bieli
 - n) Ustawienie zoomu optycznego oraz ostrości w trybie ręcznym i automatycznym
- Oprogramowanie musi umożliwiać wybór:
 - o) kompresji obrazu kamery w ramach wspieranych przez kamerę
 - p) ilości generowanych klatek na sekundę
 - q) jakości obrazu – co najmniej 10 poziomów
 - r) szybkości transmisji
 - s) rozdzielczości pracy
 - t) odstęp pomiędzy klatkami kluczowymi
- Oprogramowanie w ramach ustawienia parametryzacji pracy musi pokazywać daną chwilową przepustowość przy danych parametrach pracy kamery;
- Oprogramowanie musi umożliwiać ustawianie detekcji ruchu kamery wraz z parametryzacją czułości i progu detekcji;
- Oprogramowanie musi umożliwiać konfigurację czasu nagrywania przed i po wystąpieniu ruchu w polu widzenia kamery;
- Oprogramowanie musi umożliwiać tworzenie stref detekcji ruchu (co najmniej 5) opartych o dowolny kształt;
- Oprogramowanie musi umożliwiać konfigurację analizy wideo w kamerze (szczegółowe wymagania w dalszej części dokumentu)
- Oprogramowanie musi umożliwiać tworzenie stref prywatności w polu widzenia kamery, – co najmniej 4
- Oprogramowanie musi umożliwiać parametryzację nagrywania ręcznego (wyzwalanego przez operatora) z poziomu panelu wideo. Oprogramowanie musi umożliwiać ustawienie czasu nagrywania przed włączeniem i długości manualnego nagrywania w sytuacji włączenia go i nie wyłączenia przez operatora;
- Oprogramowanie musi umożliwiać konfigurację wejść i wyjść cyfrowych kamery (o ile kamera je posiada) oraz skutków wystąpienia danego zdarzenia dla pracy systemu nagrywania;
- Oprogramowanie musi posiadać możliwość elastycznego konfigurowania pracy

danej kamery przy użyciu kalendarza pozwalającego na wybór trybów pracy:

- Rejestracja całości materiału, ruchu, zdarzeń, brak rejestracji przy jednoczesnym podglądzie „na żywo”, itp.

3.5 Wymagania aplikacji serwerowej i klienckiej w zakresie współpracy i obsługi analizy wideo:

- Aplikacja serwerowa i kliencka musi posiadać możliwość obsługi kamer wideo z wbudowaną analizą wideo;
- Aplikacja serwerowa musi umożliwiać poprzez aplikację kliencką wyświetlanie alarmów generowanych przez daną analizę wideo wraz z zaznaczeniem na klatce miejsca zdarzenia;
- Aplikacja serwerowa musi umożliwiać korelowanie alarmów generowanych przez analizę wideo z innymi scenariuszami obsługiwanymi przez aplikację kliencką
- Aplikacja serwerowa musi umożliwiać współpracę z zewnętrznymi (niebędącymi wbudowanymi w serwerze) urządzeniami analizy wideo wraz z przesyłaniem informacji z urządzenia do serwera i aplikacji klienckiej.
- Aplikacja serwerowa i kliencka musi umożliwiać w ramach istniejącego, wbudowanego interfejsu konfigurację analiz wideo, ich pracy, oraz typów alarmów przez nie wyzwalanych

3.6 Wymagania dotyczące analizy wideo:

- Analiza wideo musi być oparta o tzw. „pattern analysis” – analiza oparta o wzorce,
- Analiza wideo musi umożliwiać analizę w oparciu o strumień wysokiej rozdzielczości, od jakości SD (kamery analogowe) do 16Mpix włącznie
- Operator musi mieć możliwość dodatkowej ingerencji w pracę algorytmów wideo – dodatkowa nauka analizy w oparciu o klasyfikację obiektów przez operatora.
- Analiza wideo musi posiadać wbudowane narzędzia do optymalizacji swojej pracy, uczenia się pracy w oparciu o otoczenie i jego charakterystykę.,
- Analiza wideo musi umożliwiać detekcję i rozróżnianie obiektów – człowiek, pojazd.
- Operator musi posiadać możliwość tworzenia stref detekcji (pracy analizy wideo) oraz stref wyjętych z analizy.
- Analiza wideo musi umożliwiać detekcję i alarmowanie w oparciu, o co najmniej niniejsze reguły: obiekt jest obecny w obszarze zainteresowania, obiekt nie jest obecny w obszarze zainteresowania, liczba obiektów przekracza dozwoloną ilość, liczba obiektów jest poniżej dozwolonej ilości, przekroczenie wirtualnej granicy przez jeden bądź kilka obiektów, pojawienie się lub zniknięcie obiektu w strefie – bez wejścia lub wyjścia ze strefy, wejście obiektu do lub wyjście obiektu z obszaru zainteresowania, wejście określonej liczby obiektów do lub wyjście określonej liczby obiektów z obszaru zainteresowania, przebywanie obiektu w obszarze zainteresowania ponad zadany czas, zatrzymanie się obiektu w obszarze zainteresowania, ruch obiektu w niedozwolonym kierunku, rozpoczęcie nagrywania w wysokiej, jakości na wypadek ruchu, zniknięcie obiektu w zaznaczonej strefie.

3.7 Wymagania w zakresie administracji systemem

- Oprogramowanie musi prowadzić log zdarzeń obejmujący następujące zdarzenia dotyczące użytkowników: logowanie, wylogowania użytkownika, serwer zmienił ustawienie, ustawienia strony zmienione, zmieniono ustawienie urządzenia, urządzenie podłączone, urządzenie odłączone, wyjście cyfrowe wyzwalone, dodanie zakładki, zakładka zaktualizowana, skasowanie zakładki, PTZ zmieniony, PTZ bezczynny, wykonanie eksport materiału o, aktywacja głośnika, głośnik wyłączony, otwarciu macierzy wirtualnej monitorów, mapa dodana, mapa aktualizowana, skasowanie mapy, widok dodany, widok zaktualizowany, widok usunięty, dodanie strony internetowej, strona internetowa zaktualizowana, strona internetowa skasowana;
- zapisywanie alarmów oraz informacji o systemie w centralnej bazie danych;
- Oprogramowanie musi prowadzić log zdarzeń obejmujący następujące zdarzenia na serwerze: uruchamianie serwera aplikacji, zamykanie serwera aplikacji, nieoczekiwana przerwa w działaniu serwera aplikacji, niski stan zasobów serwera aplikacji, błąd instalacji serwera aplikacji, licencja wkrótce wygaśnie, licencja wygasła, błąd bazy danych, błąd inicjalizacji danych, błąd partycji, powrót działania partycji, zmniejszony rozmiar do zapisu danych, błąd zapisu danych, rozpoczęcie uaktualnienia danych, aktualizacja danych zakończona, aktualizacja danych nie powiodła się, rozpoczęcie odzyskiwania danych, odzyskiwanie danych zakończone, odzyskiwanie danych nie powiodło się, zapisywanie zakładki nie powiodło się, połączenie sieciowe nawiązanie, połączenie sieciowe stracone, błąd wysyłania e-maila, błąd sprzętowy serwera, wykonywanie kopii zapasowej rozpoczęto, archiwizacja zakończona, kopia zapasowa nie powiodła się, połączenie z serwerem utracone;
- system musi zapewniać możliwość zdalnego przydzielania uprawnień dostępu przez administratorów systemu różnym lokalizacjom i serwerom z jednego miejsca;
- autoryzacja z wykorzystaniem skonfigurowanych i opisanych użytkowników wraz z możliwością importu użytkowników z domeny systemu Windows;
- możliwość niezależnego przyporządkowania uprawnień każdemu z użytkowników systemu: podgląd na żywo, sterowanie PTZ, blokowanie sterowaniem PTZ, odtwarzanie zarejestrowanego materiału, eksport materiału wideo, konfiguracja systemu, zarządzanie użytkownikami;
- funkcja raportowania o aktywności użytkownika oraz o zdarzeniach w systemie. Możliwość zapisania wyników raportu do pliku;
- Centralne zarządzanie uprawnieniami wszystkich użytkowników systemu;
- oprogramowanie musi zapewnić możliwość monitorowania dostępu użytkownika do każdego klastra serwerów;
- oprogramowanie musi zapewnić możliwość importowania i eksportowania ustawień klienta, takich jak mapy, widoki i strony internetowe;
- administracja systemu z dowolnej stacji operatorskiej włączonej do sieci komputerowej systemu monitoringu;

3.8 Mapy w systemie

- oprogramowanie musi posiadać możliwość wykorzystania wielopoziomowych,

hierarchicznych, przejrzystych map umożliwiających wskazanie zasięgu danej kamery na obiekcie;

- mapy w systemie muszą być oparte, co najmniej o pliki w formatach: jpeg, jpg, bmp, png, tiff
- oprogramowanie musi posiadać możliwość umieszczania na mapach punktów kamerowych wraz z graficznym określeniem zasięgu pola ich widzenia;
- możliwość wyboru kamery z poziomu mapy terenu;
- możliwość natychmiastowego uzyskania obrazu z wybranego punktu kamerowego poprzez kliknięcie „ikony kamery” na mapie wraz z uzyskaniem predefiniowanych obrazów z danej kamery np. sceneria ogólna wraz z jednoczesną wizualizacją wybranych miejsc w polu widzenia danej kamery (wybór z poziomu listy, mapy terenu);
- mapy muszą być aktywne tzn, pokazywać zdarzenia alarmowe w sytuacji wyzwolenia alarmu przez daną kamerę;

3.9 Sterowanie kamerami PTZ

Oprogramowaniem musi posiadać poniższe funkcjonalności, których poprawna praca będzie zależeć od poziomu integracji danej kamery z oprogramowaniem.

- oprogramowanie serwerowe i klienckie musi umożliwiać zdalne sterowanie kamerami obrotowymi (Pan/Tilt/Zoom) różnych producentów;
- oprogramowanie musi umożliwiać konfigurację co najmniej 10 programowalnych pozycji dla każdej kamery obrotowej;
- oprogramowanie musi posiadać możliwość konfigurowania tras patrolowych w kamerze obrotowej;
- oprogramowanie musi posiadać możliwość wysterowania kamery obrotowej we wcześniej zaprogramowaną pozycję presetu poprzez zdarzenie alarmowe (detekcja ruchu, alarm, itp.);
- możliwość sterowania kamerami obrotowymi przez uprawnione osoby na każdym stanowisku operatorskim w systemie za pomocą pulpitu sterującego zintegrowanego z komputerem PC i/lub konsoli wirtualnej wbudowanej w aplikację kliencką;

3.10 Eksport materiału wideo

- w ramach eksportu materiału w formacie macierzystym oprogramowanie musi umożliwiać jednoczesny eksport z jednej lub wielu kamer jednocześnie - w ramach jednego pliku do odtwarzania, z różnych przedziałów czasowych dla jednej lub wielu kamer;
- oprogramowanie musi umożliwiać określenie długości eksportowanego materiału wideo w oparciu o kalendarz jak i zaznaczenie zakresu na osi czasu;
- w ramach eksportu materiału musi istnieć możliwość wyboru wielkości generowanego pliku w zakresie: brak ograniczeń i powszechnie stosowane wielkości płyt np. CD, DVD, Blu-Ray;
- oprogramowanie musi umożliwiać konwersję materiału wideo, który został

wyeksportowany w natywnym formacie do innych popularnych formatów takich jak PNG, JPEG, TIFF, PDF;

- w ramach exportu do innego formatu niż natywny musi istnieć możliwość zmiany rozdzielczości eksportowanego pliku oraz regionu eksportu (wybranego fragmentu z całego kadru);
- funkcja dołączania programu klienckiego do oglądania nagrań eksportowanych na zewnętrzne nośniki np: CD, DVD;

3.11 Wyszukiwanie zdarzeń

- oprogramowanie musi umożliwiać przeszukiwanie zarejestrowanego obrazu i dźwięku w oparciu o różne kryteria, w tym o czas, datę, źródła wideo i zdarzenia;
- oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo na podstawie ruchu w obszarach zdefiniowanych przez użytkownika;
- oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo w oparciu o czas, datę, źródła wideo i wyświetlić wyniki jako serię miniatur;
- oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo w oparciu o zdarzenia alarmowe;
- oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo w oparciu o transakcje z urządzeń point-of-sales;
- możliwość i wsparcie programowe w aplikacji klienckiej wyszukiwania zdarzeń (dla kamer wyposażonych w analizę obrazu) w oparciu o kategoryzację obiektów jak człowiek i samochód
- Oprogramowanie musi korzystać z metadanych wyszukując zdarzeń w materiale archiwalnym. Wyszukiwanie dowodowe osób powinno zawierać minimum wyszukiwanie po kolorze górnej części ubrania, dolnej części ubrania, płci oraz kolorze włosów. Wyszukiwanie powinno odbywać się równocześnie we wszystkich kamerach dostępnych w systemie.

Alarmowanie i Obsługa alarmów

- system musi mieć możliwość generowania i eskalowania alarmów w oparciu o czas wystąpienia i priorytet;
- oprogramowanie musi umożliwiać obserwację stanu wejść alarmowych, ciągłe monitorowanie i powiadamianie (z wyświetlaniem odpowiedniego komunikatu) o każdym zaniku sygnału, zasilania, otwarciu drzwi, itp.;
- oprogramowanie musi rejestrować zdarzenia alarmowe w bazie zawierającej datę, czas wystąpienia i opis zdarzenia;
- oprogramowanie musi posiadać możliwość elastycznego kreowania reguł definiujących automatyczne reakcje systemu na dane zdarzenia (system umożliwia automatyczne reagowanie na wcześniej zdefiniowane zdarzenia i alarmy);
- możliwość stworzenia alarmów dedykowanych dla głównej stacji monitorowania (o najwyższym priorytecie);
- oprogramowanie musi posiadać możliwość wysyłania informacji o zdarzeniach poprzez e-mail;

3.12 Minimalne parametry serwerów dla rejestracji materiału z kamer

W ramach zadania planuje się zapewnić centralny zapis materiału z poszczególnych kamer przy użyciu urządzenia o poniższych parametrach technicznych:

- a) Architektura urządzenia oparta o profesjonalny serwer sieciowy – nie rejestrator sieciowy, z możliwością rozszerzenia w dowolnym momencie funkcjonowania o dodatkową przestrzeń zapisu opartą o macierz konfigurowalną w RAID 5 lub RAID 6
- b) Zainstalowane fabrycznie przez producenta serwera dyski twarde „hot swappable” typu SAS skonfigurowane w RAID 6
- c) Dwa dedykowane dyski typu „hot swappable” SATA lub SSD skonfigurowane w RAID 1 na potrzeby systemu operacyjnego oraz systemu zarządzania kamerami z funkcjami automatycznego zarządzania starzejącymi się danymi
- d) Dyski twarde pochodzące od tego samego producenta, co sam serwer
- e) Wbudowane sieciowe interfejsy co najmniej 2x10GbE SFP+ oraz 4x1GbE RJ-45
- f) Minimalna przepustowość zapisu serwera (możliwość zapisu) na poziomie co najmniej 700 Mbit/s oraz 450 Mbit/s dla odtwarzania i podglądu na żywo.
- g) Zainstalowana pamięć operacyjna na poziomie, co najmniej 16GB DDR4
- h) Zainstalowany procesor klasy i wydajności pracy nie niższej niż Intel Xeon;
- i) Wbudowane wyjścia wideo, – co najmniej 1x VGA nie służące do lokalnego oglądu kamer
- j) Preinstalowany system operacyjny klasy Windows 10 IoT Enterprise LSTB;
- k) Preinstalowana zewnętrzna karta graficzna 4Gb GDDR5, rdzenie CUDA 640, interfejs pamięci 128-bit, wyjścia miniDP 4szt.
- l) Zdalny dostęp do systemu poprzez dedykowany port RJ-45
- m) Kompaktowa obudowa 3U lub mniejsza
- n) Pojemność netto w RAID 6 – 256TB
- o) Zasilanie od 100 do 240 VAC, 50/60 Hz z autoprzejęciem
- p) Możliwość montażu drugiego zasilacza typu hot swappable”
- q) Wymaga się aby reakcja serwisowa producenta była w czasie nie gorszym niż 4 godziny.
- r) Wymaga się gwarancji na powyższych zasadach w okresie nie krótszym niż 36 miesięcy licznych od daty dostawy sprzętu do zamawiającego

3.13 KAMERA 12Mpx typu fisheye

- a) Przetwornik o minimalnej rozdzielczości 12 Mpix ze skanowaniem progresywnym o wymiarach 1/2.3”;
- b) Ilość aktywnych pikseli 2992x2992;
- c) Zakres dynamiki 81dB;
- d) Obiektyw 1.45mm o jasności F2.2;
- e) szybkość przetwarzania obrazu, co najmniej 20 klatek na sekundę włącznie przy pełnej rozdzielczości;
- f) obsługa kompresji obrazu: H.264, MJPEG;
- g) minimalne natężenie światła: 0,49 lux dla F2.2 w trybie kolorowym; 0 dla F2.2 lux w trybie monochromatycznym przy włączonym IR;
- h) Wbudowany promiennik podczerwieni o zasięgu do 10m;

- i) automatyczny tryb dzień/noc;
- j) automatyczna i ręczna regulacja balansu bieli;
- k) co najmniej jedno wejście i jedno wyjście alarmowe;
- l) minimum 64 strefy prywatności;
- m) możliwość zasilania poprzez: 12 V lub 24 V (AC lub DC) i PoE (IEEE802.3af) lub PoE+ (IEEE802.3at);
- n) Temperatura pracy od -40 °C to +55 °C;
- o) Zasilanie awaryjne RTC baterią 3V
- p) standard interfejsu sieciowego: co najmniej 100BASE-TX;
- q) Zgodność ze standardem Analytics Service Specification w wersji 1.02, 2.00, Profile S i 2.2.0 opracowanym przez stowarzyszenie ONVIF
- r) Gwarancja 36 miesięcy;

3.14 KAMERA ZEWNĘTRZNA 16MP

- a) Przetwornik CMOS 27,2mm o minimalnej rozdzielczości 16 Mpix ze skanowaniem progresywnym o wymiarach 23,6 mm (w poziomie) x 13,4 mm (w pionie); 0,93" (w poziomie) x 0,53";
- b) Ilość aktywnych pikseli 4944x3280;
- c) Zakres dynamiki 70dB;
- d) Obiektyw, wymienne obiektywy z mocowaniem EF lub EF-S;
- e) szybkość przetwarzania obrazu, co najmniej 10 klatek na sekundę włącznie przy pełnej rozdzielczości;
- f) obsługa kompresji obrazu: H.264, MJPEG;
- g) minimalne natężenie światła: 0,005 lux dla F1.4 w trybie kolorowym;
- h) dostępna z poziomu oprogramowania kamery możliwość sterowania ostrością wsparta funkcją autofocus;
- i) automatyczny tryb dzień/noc;
- j) automatyczna i ręczna regulacja balansu bieli;
- k) co najmniej jedno wejście i jedno wyjście alarmowe;
- l) minimum 4 strefy prywatności;
- m) Kamera powinna obsługiwać protokoły: IPv6, IPv4, HTTP, HTTPS, SOAP, DNS, NTP, RTSP, RTCP, RTP, TCP,UDP, IGMP, ICMP, DHCP, Zeroconf, ARP
- n) możliwość zasilania poprzez: 12 V lub 24 V (AC lub DC) i PoE (IEEE802.3af) lub PoE+ (IEEE802.3at);
- o) standard interfejsu sieciowego: co najmniej 100BASE-TX;
- p) obudowa zewnętrzna o klasie szczelności IP66, umożliwiająca pracę kamery w zakresie temperatur od -30 °C do +50 °C;
- q) Kamera powinna być wyposażona w algorytmy samouczącej się analizy obrazu w oparciu o klasyfikację obiektów(np. człowiek, pojazd) z przesyłaniem metadanych na serwer:
 - Obiekty na obszarze;
 - Podejrzane zachowanie obiektu;
 - Przekroczenie wiązki detekcyjnej przez obiekty;
 - Pojawienie się obiektu lub znalezienie się obiektu na obszarze;
 - Obiekt nieobecny na obszarze;

- Znalezienie się obiektów na obszarze;
 - Opuszczenie obszaru przez obiekty;
 - Zatrzymanie się obiektu na obszarze;
 - Niedozwolony kierunek;
 - Wykrycie ingerencji;
- r) Kamera powinna umożliwiać stworzenie nie mniej niż 14 reguł alarmowych z algorytmów analizy obrazu działających równolegle bez utraty funkcjonalności pozostałych parametrów kamery.
- s) Zgodność ze standardem Analytics Service Specification w wersji 1.02, 2.00, Profile S i 2.2.0 opracowanym przez stowarzyszenie ONVIF
- t) Gwarancja 36 miesięcy;

3.15 OBIEKTYW do kamer 16MP

- a) Obiektyw zmiennoogniskowy 24-70mm
- b) Kąt widzenia 84°-34°
- c) Liczba listków przysłony – 9
- d) Maksymalna Przysłona f/2.8
- e) Minimalna przysłona f/22
- f) Dostępna stabilizacja obrazu
- g) Elektroniczne sterowanie autofocusem

3.16 KAMERA DOME 6MPX

- a) Przetwornik o minimalnej rozdzielczości 6 Mpix ze skanowaniem progresywnym o wymiarach 1/1.8”;
- b) Ilość aktywnych pikseli (16:9) 3200 × 1800 (3:2) 3072 × 2048;
- c) Zakres dynamiki 120dB;
- d) Obiektyw minimum 4,9-8mm o jasności F1.8 ze sterowaniem P-IRIS;
- e) szybkość przetwarzania obrazu, co najmniej 30 klatek na sekundę włącznie przy pełnej rozdzielczości;
- f) obsługa kompresji obrazu: H.264, MJPEG;
- g) minimalne natężenie światła: 0,055 lux dla F1.3 w trybie kolorowym; 0,028 lux w trybie monochromatycznym, 0 lux przy włączonym reflektorze IR;
- h) zmiennoogniskowy obiektyw z funkcjami motozoom i autofocus;
- i) dostępna z poziomu oprogramowania kamery możliwość regulacji ogniskowej;
- j) dostępna z poziomu oprogramowania kamery możliwość sterowania ostrością wsparta funkcją autofocus;
- k) automatyczny tryb dzień/noc;
- l) automatyczna i ręczna regulacja balansu bieli;
- m) co najmniej jedno wejście i jedno wyjście alarmowe;
- n) minimum 64 strefy prywatności;
- o) możliwość zasilania poprzez: 12 V lub 24 V (AC lub DC) i PoE (IEEE802.3af) lub PoE+ (IEEE802.3at);
- p) standard interfejsu sieciowego: co najmniej 100BASE-TX;

- q) obudowa zintegrowania z promiennikiem podczerwieni;
- r) Zintegrowany doświetlacz IR pracujący w paśmie 850nm o zasięgu nie mniejszym niż 30m, niepowodujący zakłóceń innych urządzeń;
- s) Kamera powinna być wyposażona w algorytmy samouczącej się analizy obrazu w oparciu o klasyfikację obiektów (np. człowiek, pojazd) z przesyłaniem metadanych na serwer:
 - Obiekty na obszarze;
 - Podejrzane zachowanie obiektu;
 - Przekroczenie wiązki detekcyjnej przez obiekty;
 - Pojawienie się obiektu lub znalezienie się obiektu na obszarze;
 - Obiekt nieobecny na obszarze;
 - Znalezienie się obiektów na obszarze;
 - Opuszczenie obszaru przez obiekty;
 - Zatrzymanie się obiektu na obszarze;
 - Niedozwolony kierunek;
 - Wykrycie ingerencji;
- t) Kamera powinna umożliwiać stworzenie nie mniej niż 14 reguł alarmowych z algorytmów analizy obrazu działających równolegle bez utraty funkcjonalności pozostałych parametrów kamery.
- u) Zgodność ze standardem Analytics Service Specification w wersji 1.02, 2.00, Profile S, T i 2.2.0 opracowanym przez stowarzyszenie ONVIF
- v) Gwarancja 60 miesięcy;

3.17 Stacja robocza z monitorami

- a) Procesor Intel Core i7 min. 3Ghz
- b) Pamięć 8 GB DDR4 RAM
- c) Interfejs sieciowy 2 x 1Gbe RJ45
- d) Windows 10 IoT
- e) Wyjścia wideo 4xDP (wsparcie rozdzielczości 4x4K)
- f) Wsparcie monitorów – do 4ch monitorów podłączonych bezpośrednio
- g) Obudowa typu monitower
- h) Możliwość wyświetlenia do 140 obrazów z kamer równocześnie
- i) Stacja robocza dostarczona z monitorami 32" o rozdzielczości 4K/UHD

Uwaga:

W celu utrzymania standardu HD, sprawdzić czy napięcie w punkcie przyłączenia kamery mieści się w granicach $Un \pm 3\%$.

3.18 NASYCENIE PIXELI

Nasylenie pixelami w systemie CCTV, nie może być mniejsze niż 150px/m.

3. SYSTEM PRZYWOŁANIA

System przywołania zainstalowany zostanie w toaletach dla niepełnosprawnych.

System składa się z:

- Terminala łazienkowego
- Terminala pokojowego
- Czytnika resetowania alarmu

4.1 Terminal łazienkowy

Urządzenie pozwalające na wysyłanie sygnału SOS do terminala.

- przycisk pociągowy do wywołania alarmu przez osobę przebywającą w łazience
- Zasilanie: 12 VDC

4.2 Terminal pokojowy

Terminal pokojowy, pozwala na wysyłanie alarmów do koncentratora poprzez sieć.

Urządzenie posiada 4 wejścia alarmowe oraz wejście Reset.

- 3 wejścia alarmowe
- 1 wejście do podłączenia łazienkowego przycisku pociągowego
- interfejs
- programowanie poprzez dip-switch
- Zasilanie: 12 VDC

4.3 Czytnik resetowania alarmu

Urządzenie do resetowania alarmów.

- resetowanie alarmów za pomocą karty

4. INSTALACJA SSWiN

Projektowany system sygnalizacji włamania i napadu oparty jest o urządzenia:

- Klawiatura dotykowa sensoryczna z wyświetlaczem LCD
- Zintegrowany Kontroler Systemowy
- Moduł rozszerzenia 16 wejść
- Inteligentny zasilacz systemowy wersja DIN 4A
- Obudowa na szynę DIN
- Sygnalizator wewnętrzny akustyczny
- Sygnalizator zewnętrzny akustyczno/optyczny
- Czujka pasywnej podczerwieni
- Czujka dualna z antymaskingiem

5.1 Klawiatura dotykowa sensoryczna z wyświetlaczem LCD

Zasilanie	
Napięcie zasilania	11.0 VDC do 14.0 VDC
Pobór prądu	60mA (95mA Max)
Komunikacja	
RS-485	Szyfrowana magistrala komunikacji modułów
interfejs użytkownika	
Wyświetlacz	LCD 16 x 2, wyświetlacz alfanumeryczny, inteligentne zarządzanie podświetlaniem
Klawiatura	23 przyciski klawiatury dotykowej, 3 diody statusu w pełni programowalne
Wejścia	
Sabotaż	Wbudowany mikro wyłącznik sabotażowy oderwania od ściany i otwarcia urządzenia
Wejście problem	2 standardowe wejścia alarmowe, 4 w trybie duplex
Wyjścia PGM	
Wyjścia PGM	1 wyjście otwarty Kolektor, 50mA max, dowolnie programowalne
Diody LED	3 diody LED do dowolnego zaprogramowania
Temperatura	
Temperatura Pracy	0°C ÷ 49°C
Temperatura przechowywania	-10°C ÷ 85°C
Wilgotność	0% ÷ 93% nie skondensowana, tylko do pracy wewnątrz budynków (wilgotność względna)

5.2 Zintegrowany Kontroler Systemowy

Napięcie zasilania	12V DC ± 10%
Pobór prądu	120mA (typowy)
Wyjście zasilające DC AUX	0.7A (typowo), elektroniczne odcięcie przy 1.1A
Wyjście syreny (ciągłe)	8 Ohm 30W lub 1.1A (typowo)
Wyjście syreny (chwilowo)	1500mA
Całkowity prąd*	3.4A (max)
Elektroniczne odłączenie	9.0 V DC
Komunikacja Ethernet	Port komunikacyjny 10/100Mbps
Komunikacja szeregową	Port komunikacyjny RS-485
Komunikacja modem	Wbudowany modem 2400bps
Porty czytników	2 porty Wiegand lub ClockData pozwalające na obsługę 2 przejść jednostronnych lub 2 przejść dwustronnych

Wejścia	8 wejść wysokiego zabezpieczenia
Wyjścia OC	4 wyjścia Otwarty Kolektor 50mA, dla obsługi czytników, lub innych funkcji
Wyjścia przekaźnikowe	2 wyjścia z przekaźnikami FORM-C, 7A max
Temperatura Pracy	0°C ÷ 49°C
Temperatura przechowywania	-10°C ÷ 85°C
Wilgotność	0% ÷ 85% nie skondensowana, tylko do pracy wewnątrz budynków (wilgotność względna)

5.3 Moduł rozszerzenia 16 wejść

Zasilanie	
Napięcie zasilania	12V DC ± 10%
Pobór prądu	80mA (typowy)
Niskie napięcie odcięcia	8.7V DC
Niskie napięcie powrót	10.5V DC
Komunikacja	
RS-485	Szyfrowana magistrala komunikacji modułów
Wejścia	
Wejścia alarmowe	16, szybkość działania programowalna w zakresie od 10ms do 1 h osobno dla każdego wejścia)
Sabotaż	1 (NC)
Wejście problem	16
Temperatura	
Temperatura Pracy	5°C ÷ 55°C
Temperatura przechowywania	-10°C ÷ 85°C
Wilgotność	0% ÷ 85% nie skondensowana, tylko do pracy wewnątrz budynków (wilgotność względna)

5.4 Zasilacz systemowy 4A

Zasilanie	
Napięcie wejściowe AC	90 - 264Vac, 47 – 63Hz
Pobór prądu	1500mA przy 120Vac podczas pełnego obciążenia
Wyjścia DC razem	12.64dc 4A razem z wyjść V1out i V2out
Pojedyncze Wyjście DC	12.2Vdc 3A Max
Ładowanie baterii	500mA (typowo)
Niskie napięcie baterii	10.5 V DC
Niskie napięcie baterii powrót	11.5 V DC

Elektroniczne odłączenie baterii	9.4 V DC
Komunikacja	
RS-485	Szyfrowana magistrala komunikacji modułów, galwanicznie izolowana
Wejścia	
Sabotaż	1 (NC)
Wejście problem	8
Wyjścia PGM	
Wyjścia PGM	2 wyjścia w formie przekaźników elektronicznych Solid State, 12V/50mA max
Temperatura	
Temperatura Pracy	0°C ÷ 49°C
Temperatura przechowywania	-10°C ÷ 85°C
Wilgotność	0% ÷ 93% nie skondensowana, tylko do pracy wewnątrz budynków (wilgotność względna)

5.5 Obudowa na szynę DIN

Metalowa obudowa I jest zaprojektowana specjalnie dla modułów wykonanych w formie urządzeń do montażu na szynę DIN.

Obudowa posiada zamontowane dwa rzędy szyny DIN pozwalające na montaż maksymalnie 4 modułów DIN.

Obudowa wyposażona jest w:

- Szyny DIN do montażu maksymalnie 4 modułów DIN
- Styk antysabotażowy otwarcia obudowy
- Styk antysabotażowy oderwania obudowy od ściany
- Zamek

5.6 Sygnalizator wewnętrzny akustyczny

Podstawowe parametry sygnalizatorów:

- Zewnętrzna obudowa wykonana z poliwęglanu o wysokiej odporności mechanicznej.
- Ciśnienie akustyczne: 100dB(A)
- Częstotliwość dźwięku: 3500 – 3700 Hz .
- Zabezpieczenie przed odwrotną polaryzacją zasilania z akumulatora i z centrali alarmowej.
- Zabezpieczenie antysabotażowe przed otwarciem obudowy i zdjęciem ze ściany.
- Napięcie zasilania: 12 lub 24Vdc
- Pobór prądu: max 260 mA (podczas alarmu)

5.7 Sygnalizator zewnętrzny akustyczno/optyczny

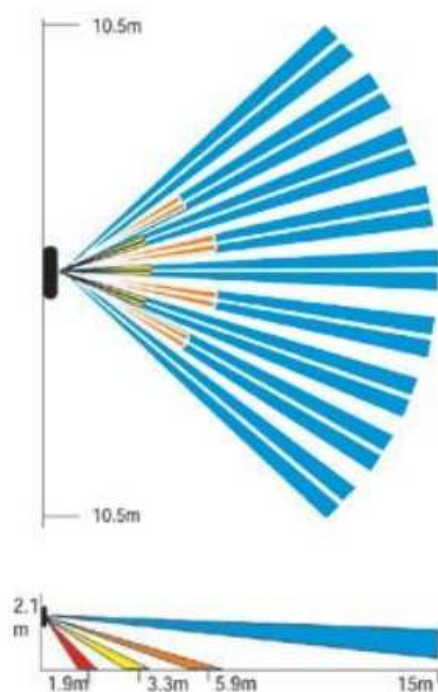
Podstawowe cechy sygnalizatorów:

- Funkcja służąca do przesłuchania 16 różnych sygnałów dźwiękowych (przy zmniejszonej mocy).
- Zabezpieczenie przed odwrotną polaryzacją zasilania z akumulatora i z centrali alarmowej.
- Możliwość zaprogramowania wejść blokujących BC i TC jako zbalansowane lub normalnie zamknięte oraz odniesienia potencjału do + lub -.
- Programowany czas trwania alarmu w przypadku gdy nie ma sygnału blokowania (4 różne tryby).
- Opcjonalnie: dodatkowa wewnętrzna osłona metal, detekcja pianki-przekroczenia temperatury-wykrywanie przewiercenia obudowy
- Elektryczne wyjście awaryjne gdy rozładowuje się bateria, wystąpi zwarcie na module świetlnym lub dźwiękowym lub anomalia w module zabezpieczenia (jeśli jest obecny).
- Zabezpieczenie antysabotażowe przed otwarciem obudowy i zdjęciem ze ściany.
- Kontrola pobieranego prądu przez jednostkę centralną (ograniczenie do 150 mA).
- Licznik sygnałów dźwiękowych (można wyłączyć).
- Test baterii (podczas ładowania), lampy oraz syreny.
- Lampa w technologii LED.
- Sterowanie mikroprocesorowe.
- Sygnalizacja pamięci alarmów (za pomocą migającej lampy).

5.8 Czujka pasywnej podczerwieni

GŁÓWNE CECHY:

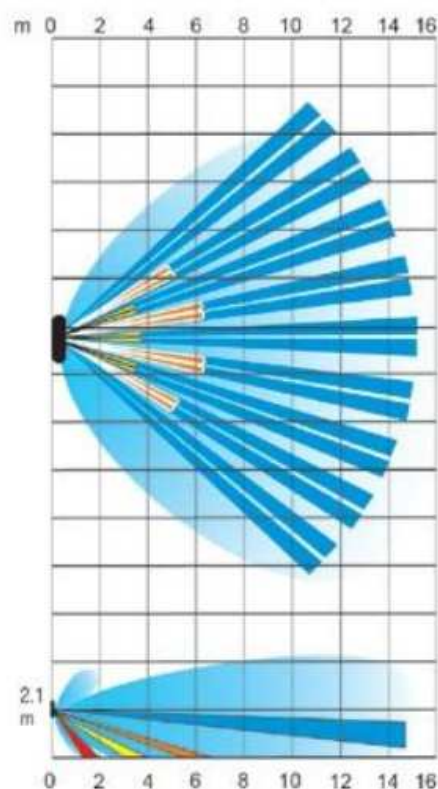
- Cyfrowa wolumetryczna czujka z czujnikiem pasywnej podczerwieni (PIR)
- Dwa regulowane poziomy czułości
- Max zasięg 15 m
- Kąt detekcji 90°
- Soczewki Fresnela: 18 wiązek na 4 płaszczyznach ze strefą podejścia
- Zasilanie: 12V +/- 3V
- Pobór prądu: 13 mA nom ~ 17 mA max
- Przekaznik: 100mA / 24V
- Sabotaż: 100 mA / 30V
- Wilgotność: 95%
- Temperatura pracy: -10°C - +55°C
- uchwyt do montażu ściennego lub sufitowego



5.9 Czujka dualna z antymaskingiem

PARAMETRY TECHNICZNE:

- Urządzenie zawierające czujniki pasywnej podczerwieni (PIR) oraz mikrofalowe (MW)
- Max zasięg 15 m
- Kąt detekcji czujnika MW: 90° poziomo - 36° pionowo
- Kąt detekcji PIR: 90°
- Strefy detekcji: 18 na 4 płaszczyznach ze strefą podejścia
- Możliwość zablokowania diody LED
- Zasilanie: 12V +/- 3V
- Pobór prądu: 20 mA nom ~ 34 mA max
- Czujnik MW z regulacją zasięgu
- Częstotliwość czujnika MW: 10.525 GHz
- Emisja fal MW (EIRP): 8 dBm
- Przekaznik: 100mA / 24V
- Sabotaż: 100 mA / 30V
- Temperatura pracy: -10°C - +55°C
- Uchwyty do montażu ściennego lub sufitowego



Zintegrowany System Bezpieczeństwa i Automatyki Budynku jest wysoko skalowalną platformą oferującą zintegrowany system bezpieczeństwa dla obiektu, z możliwością realizacji funkcji automatyki budynkowej oraz z szerokimi możliwościami integracji z zewnętrznymi systemami (jak np. systemy BMS, serwery OPC, systemy sterowania windami, systemy klasy ERP, SCADA, HVAC, i inne). Skalowalna i modułowa koncepcja systemu sprawia, że jest odpowiedni dla wszystkich – od małych systemów z pojedynczymi drzwiami do wielkich międzynarodowych korporacji, z wieloma lokalizacjami na całym świecie. Wysoce zintegrowane kontrolery systemowe oparte na mikroprocesorach 32 bitowych oraz opcjonalne moduły rozszerzeń zapewniają adaptacyjny system o najwyższej funkcjonalności i ogromnych możliwościach rozwoju.

Najważniejsze właściwości

- Architektura klient – serwer z funkcjami kontroli i monitoringu online
- Intuicyjny i przyjazny dla użytkownika interfejs z interaktywną graficzną wizualizacją systemu oraz niezwykle łatwymi w użyciu i dostosowywaniu do swoich potrzeb Stronami Statusu dla kontroli i monitorowania
- Zaawansowany generator raportów, z możliwością utworzenia niezliczonej ilości własnych raportów i filtrów dostosowanych do własnych potrzeb, z przyjaznym i łatwym w użyciu kreatorem
- Filtry alarmów i zdarzeń, pozwalają na przejrzyste sortowanie i kategoryzowanie zdarzeń, łatwe zarządzanie wyświetlaniem zdarzeń, alarmów i innych danych
- Wysoko wydajna baza danych Microsoft SQL Server®
- Możliwość podziału systemu na wiele odrębnych instalacji / systemów pracujących na tym samym serwerze
- Integracja użytkowników i operatorów za pomocą protokołu LDAP (Active Directory)

- Możliwość pracy wielomonitorowej za pomocą odłączanych okien od programu głównego

Intuicyjny Interfejs Użytkownika

Interaktywne mapy wizualizacji oraz Strony Statusów dostarczają intuicyjnego interfejsu graficznego do kontroli i monitorowania systemu. Wyświetlaj informacje odpowiednie do własnych potrzeb, pochodzące z Twojego systemu, a nie z części instalacji należącej do sąsiada!

Strony Statusów

W pełni dostosowywane do własnych potrzeb Strony Statusów są jedną z flagowych funkcji systemu i mogą być dopasowane do wyświetlania dokładnie takich informacji jakich potrzebujesz! **Strony Statusów** mogą zawierać dowolne kombinacje następujących elementów:

- **Listy Statusów**, które dynamicznie aktualizują (w trybie online) rzeczywisty status wybranych urządzeń
- **Interaktywne Mapy Wizualizacji**, będące graficzną reprezentacją systemu lub jego części, wyświetlają online rzeczywisty stan urządzeń i obiektów w systemie
- **Obrazy z Kamer** na żywo, pochodzące ze zintegrowanych systemów DVR/NVR
- **Zdarzenia**, filtrowane w oknach, tak aby otrzymywać posegregowane i uporządkowane zdarzenia odpowiednie dla własnych potrzeb
- **Zmienne**, pokazujące zmieniające się dane (najczęściej z kanałów analogowych, lub dane zewnętrzne) takie jak np. temperatura w pomieszczeniu, wilgotność, itp.
- **Raporty** ewakuacyjne dostarczające aktualnych danych na temat wszystkich użytkowników w zdefiniowanych strefach
- **Intuicyjny interfejs graficzny** minimalizuje czas uczenia się obsługi, pozwala na korzystanie z systemu przez nowych użytkowników sprawnie i szybko
- **Elastyczna konstrukcja** pozwala na wyświetlanie danych odpowiednich dla każdego operatora z osobna
- **Dopasuj rozkład elementów** do własnych potrzeb. Ekran można podzielić na 16 pól, o dowolnym układzie, w siatce 4x4.
- **Zyskaj ogólny obraz** swojego systemu. Kliknij aby wejść głębiej i zobaczyć szczegóły. Wysoka elastyczność pozwala na łatwe dopasowanie interfejsu do własnych potrzeb i sposobu działania.

Interaktywne Mapy Wizualizacji

Interaktywne Mapy Wizualizacji prezentują graficzne odzwierciedlenie instalacji oraz są szybką i efektywną metodą kontroli i monitorowania systemu.

Możesz szybko uzbroić i rozbroić strefy, obserwować ich stan, kontrolować drzwi i wyjścia, obserwować status wejść oraz informacje o zmiennych – wszystko w trybie rzeczywistym.

- Graficzne ikony, wbudowane lub własne
- Przyciski „drag and drop” pozwalające na łatwą nawigację pomiędzy mapami, a także obrazami z kamer na żywo
- Wyświetlanie statusu urządzeń i obiektów w czasie rzeczywistym
- Zmienne, pokazujące zmieniające się dane (najczęściej z kanałów analogowych, lub dane zewnętrzne) takie jak np. temperatura w pomieszczeniu, wilgotność, itp.

Moduły oprogramowania

Oprogramowanie systemu składa się z podstawowego modułu serwera oraz dodatkowych modułów rozszerzających

właściwości i funkcjonalność systemu. Poniżej przedstawione są obecne na ta chwilę moduły oprogramowania. System

jest systemem ciągle rozbudowywanym gdzie lista dostępnych modułów oprogramowania jest ciągle rozszerzana.

5. INSTALACJA KD

Kontroler jest modułem interfejsu IP i elastyczną obsługą, umożliwiającą podłączenie szerokiej gamy urządzeń zabezpieczających. Kontroler jest łatwy w instalacji i zapewnia wymagane wejścia / wyjścia do łączenia czterech czytników kontroli dostępu przy użyciu protokołu OSDP, sześć wejściowych ogólnego przeznaczenia i czterech wyjść sterujących do dowolnego inteligentnego kontrolera z serii pasującej do kontrolera.

Kontroler to moduł interfejsu z obsługą IP z elastycznością pokładową do łączenia szerokiej gamy urządzeń zabezpieczających. Kontroler jest łatwy w instalacji i zapewnia wymagane I / O do łączenia czterech czytników kart przy użyciu protokołu OSDP, sześć uniwersalne punkty monitorowania wejść i cztery przekaźniki sterowania do dowolnego inteligentnego sterownika serii pasującej do niego. Kontroler zapewnia zwiększoną moc wyjściową przy użyciu PoE + i zapewnia jeden port czytnika obsługującego protokół OSDP Secure

Główne cechy:

- Wsparcie protokołu OSDP
- Zwiększone bezpieczeństwo: Wbudowany układ pamięci kryptograficznej zapewnia bezpieczną warstwę szyfrowania w celu ochrony poufnych danych
- Moduł wejścia/wyjścia z obsługą zasilania PoE +
- Zapewnia 1,5A mocy
- IPv4/6
- Komunikacja zabezpieczona przez TLS 1.2/1.1 lub AES-256/126
- Dostępne certyfikaty dla TLS
- FIPS 140-2 dla Open SSI
- Kontrola dostępu sieciowego 802.1X
- Zerconf Device Discovery (mDNS)
- Obsługa czytników po protokole OSDP, wsparcie wielu formatów kart, czytników biometrycznych, wind itp.

Specyfikacja techniczna:

Kontrola drzwi	Wsparcie do 4ch czytników. Nie wspiera czytników Wiegand . AC-MER-RIM-MR62E, podłączone do kontrolera wspiera do 2ch drzwi.
Format kart	Wsparcie 8 formatów kart.Karty 19 znakowe(64 bit), User ID 15 znaków PIN. Kompatybilność kart PIV, CAC, TWIC
Zasilanie wej.	PoE (12.95 W), compliant to IEEE 802.3af or PoE+ (25 W), compliant to IEEE 802.3at or 12 Vdc \pm 10 %, 1.7 A maximum
Zasilanie wyj.	PoE: zamki I czytniki, współdzielone: 12 Vdc .66 A MAX, PoE+ lub 12 Vdc: zamki 12

	Vdc @ 1 A MAX, czynniki 12 Vdc @ .5 A MAX
Wyjścia	4 przełączniki, 2 A @ 30 Vdc
Wejścia	6 nadzorowanych/nienadzorowanych, EOL, 1k/1k ohm
Zasilanie	12 Vdc @ .5 A MAX
Komunikacja	2-przewodowy RS-485, protokół OSDP,
Temperatura	-55 to 85 °C przechowywanie, 0 do 70 °C, praca
Wilgotność	5 to 95% RHNC
Wymiary	5.5 in. (140 mm) W x 2.75 in. (70 mm) L x 0.96 in. (24 mm) bez uchwytu 5.5 in. (140 mm) W x 3.63 in. (92 mm) L x 1.33 in. (34 mm) H z uchwytem
Waga	(112 g) bez uchwytu (142 g) z uchwytem
Certyfikaty	UL294*, FCC Część 15 Class A, CE, RoHS, NIST

6.1 KONTROLER GŁÓWNY

Wieloportowy kontroler pozwala na sterowanie dwoma drzwiami podłączonymi bezpośrednio do płyty głównej oraz dodatkowo rozszerzyć do max. 64 przejść kontrolowanych za pośrednictwem modułów rozszerzających. Natywna komunikacja, wysoka wydajność kontrolera sprawia, że działa niezależnie od ilości połączonych hostów aplikacji do kontroli dostępu. Obsługuje OSDP, bezpieczny OSDP, klawiatury, czynniki biometryczne, Wiegand, zegar i dane, paski magnetyczne , F / 2F i nadzorowane technologie czytnika F / 2F.

Główne cechy:

- Zwiększone bezpieczeństwo: Wbudowany układ pamięci kryptograficznej i szyfrowanie danych zapewniają bezpieczną warstwę ochrony poufnych danych
- Protokół OSDP: Bezpieczna komunikacja pomiędzy kontrolerem a czytnikiem
- Komunikacja hosta chroniona przez TLS 1.2 / 1.1
- Złącze rozszerzające kontroler / IO chronione przez AES
- Kontrola dostępu do sieci za pomocą 802.1X
- Wsparcie dla OpenSSL
- Obsługa czytników po protokołach OSDP, wsparcie wielu formatów kart, czytników biometrycznych, wind, itp.
- Funkcja Anti-passback

Parametry techniczne

Kontrola dostępu	189,486 pojemność kart 50,000 bufor transakcji Wsparcie protokołu RS-485 IO protokołów 16 poziomów dostępu dla posiadacza kart Karta- 19 znaków (64 Bit) User ID z 8 znakami naPIN MAX	Wsparcie anypasback Zagnieżdżanie, obszar, twarde, softowe i czasowe dopasowanie kart Wsparcie do 504 wejść lub 500 wyjść
------------------	---	--

Kontrola drzwi	Natywne wsparcie do 4 czytników. Rozszerzenie do 64 czytników
Zasilanie	12 to 24 Vdc \pm 10 %, 500 mA max
Port czytników	600 mA max
Mico USB	5 Vdc, 500 mA max
Bateria	Pamięć/backup: 3 Volt Lithium, typ BR2330 lub CR2330
Karta microSD	microSD lub microSDHC; 2GB do 8GB
Komunikacja hosta	Ethernet: 10-BaseT/100Base-TX lub USB port (2.0) z adapterem USB2-OTGE100
Urządzenia I/O	2-przewody RS-485, 2,400 do 115,200 bps, asynchronicznie, półdupleks, 1 start bit, 8 bit data, 1 stop bit
Wejścia	8 nadzorowanych/nienadzorowanych, EOL: 1k/1k ohm, 1%, ¼ watt. Dwa nienadzorowane wejścia tamper
Wyjścia	4 przełączniki, Z C, NO 5 A @ 30 Vdc, NC 3 A @ 30 Vdc
Zasilanie czytnika	12-24 Vdc \pm 10 % regulowane, 300 mA max. każdy
Wejście danych	TTL kompatybilność, F/2F lub 2-przewody RS-485
RS-485	9,600 to 115,200 bps asynchronicznie, półdupleks, 1 start bit, 8 bit data, 1 stop bit. Max. dystans kabla: (609.6 m)
Wyjście LED	Poziom TTL, wysoki >3 V, niski <0.5 V, 5 mA źródło
Wyjście Buzzer	Open collector, 12 Vdc obwód otwarty maximum,
Zasilanie i czytniki	1 para skrętka, 18 do 16 AWG
Ethernet	CAT-5, min.
Czytnik TTL	6-przewodnikowy, 18 AWG, (150 m)
Czytnik F/2F	4-przewodnikowy, 18 AWG, (150 m)
Czytnik RS-485	1 para skręcona, ekranowana, 120 ohm impedancja, 24 AWG, (610 m) max.
Urządzenia I/O	1 skręcona para ekranowana, 120 ohm impedancja, 24 AWG, (1,219 m) max
Wejścia alarmowe	1 skręcona para, 30 ohm max
Temperatura	-55 to 85 °C przechowywanie, 0 to 70 °C, praca
Wilgotność	5 to 95% RHNC
Wymiary	(203.2 mm) W x (152.4 mm) L x (25 mm) H
Waga	(255 g) nominalnie, płyta
Certyfikaty	UL294, FCC Część 15 Klasa A, CE, RoHS, NIST szyfrowanie

6. System AV

8.1 Spis oznaczeń

Oznaczenie	Opis
AMP 100V	Wzmacniacz 100V
AMP	Wzmacniacz stereo
BLURAY	Odtwarzacz Bluray
DSP	Procesor DSP
EKRx	Ekran elektryczny
GSx	Głośnik sufitowy
J.CENTR	Jednostka centralna systemu sterowania
MIKR.x	Mikrofon bezprzewodowy
PROJ	Projektor
RACK AV	Szafa rackowa AV
PSTx	Przylącze sygnałowe stołowe
ROUTER	Router bezprzewodowy
SW.HDMI	Przełącznik HDMI
ZGL	Zestaw głośnikowy ścienny, lewy
ZGP	Zestaw głośnikowy ścienny, prawy

8.2 Sala konferencyjna 2.15

a) System projekcji

Dla sali konferencyjnej przewidziano system projekcji złożony z ekranu o szerokości 240cm i współpracującego z nim projektora laserowego o rozdzielczości WUXGA (1920x1200) i jasności 5000lumenów. Tubus ekranu zostanie zamocowany w suficie podwieszanym.

Projektor będzie zamocowany na uchwycie pod sufitem podwieszanym. Sterowanie ekranem, projektorem odbywać się będzie zdalnie przez centralny system sterowania.

Projektor będzie umożliwiał prezentację multimedialną z następujących źródeł audio-wideo:

- Laptop użytkownika lub inne źródło – podłączane do systemu w standardzie HDMI do przyłączy stołowych PST1 – PST8

Wybór źródła prezentacji dokonywany będzie zdalnie z poziomu systemu sterowania – poprzez wybór opcji prezentacji na panelu dotykowym.

W systemie przewidziano przełącznik HDMI 4:1 (z deembedowaniem sygnału audio).

b) System nagłaśniający

Na potrzeby prezentacji multimedialnych zaprojektowano system nagłośnienia. System będzie składał się z sześciu głośników sufitowych, wzmacniacza 100V, procesora fonicznego DSP oraz mikrofonów bezprzewodowych.

Podstawową funkcją systemu nagłośnienia ogólnego jest transmisja sygnału mowy i dźwięku towarzyszącego prezentacjom multimedialnym.

Głównym elementem systemu nagłaśniającego będzie programowalny procesor foniczny DSP. Procesor będzie wyposażony w miksery, matryce audio, układy antysprężeniowe, korektory barw, limityry, kompresory.

Do procesora będą podłączone źródła dźwięku (mikrofony, muzyka, dźwięk z prezentacji) oraz na wyjściu wzmacniacz z głośnikami.

Do dyspozycji mówców będą 2 mikrofony bezprzewodowe typu „handheld” – 2 szt. trzymane w ręku lub stawiane na statywie stołowym.

c) System centralnego sterowania

Dla zapewnienia łatwej obsługi systemu audiowizualnego zastosowano system zintegrowanego sterowania, który umożliwi sterowanie urządzeniami AV oraz wyposażeniem elektrycznym sali.

Elementem sterującym będzie bezprzewodowy ekran dotykowy o przekątnej 10”.

Układ graficzny ekranu zostanie opracowany na etapie instalacji i uruchomienia systemu. Za pośrednictwem ekranu będzie można sterować poszczególnymi urządzeniami (projektorem, ekranem, nagłośnieniem, roletami). Można będzie również uruchamiać sekwencje czynności.

Głównym elementem zarządzającym systemem będzie jednostka centralna w pamięci której zaimplementowany będzie program obsługi systemu audiowizualnego sali. Z

jednostką centralną umieszczoną w szafie rackowej współpracują moduły wykonawcze zamontowane w rozdzielni elektrycznej, odpowiedzialne za sterowanie ekranem, roletami.

d) Szafa RACK

Szafa rackowa AV z urządzeniami systemu AV umieszczona będzie w rogu pomieszczenia.

8.3 Wytyczne dla branżystów

a) Rozdzielnica elektryczna i AV – branża elektryczna

Tablica elektryczna dla pomieszczenia 2.15 będzie znajdowała się na w pomieszczeniu 2.4. Sama tablica elektryczna wraz z zabezpieczeniami oraz elementami końcowymi sterowania oświetlenia (jak styczniki) jest ujęta w opracowaniu branży elektrycznej i oświetleniowej.

W rozdzielni będą znajdowały się moduły przekaźnikowe do obsługi rolet, ekranów elektrycznych oraz zabezpieczenia nadprądowe urządzeń audiowizualnych.

Należy doprowadzić zasilanie do urządzeń AV: szaf rackowych AV, projektorów, ekranów elektrycznych, przyłączy sygnałowych stołowych i odpowiednio zabezpieczyć.

Linie zasilające będą posiadały stosowne zabezpieczenia różnicowoprądowe i przeciwprzepięciowe zgodnie z obowiązującymi przepisami.

Dobór opraw i ich rozmieszczenie nie jest przedmiotem projektu a/v a projektu elektrycznego. Oświetlenie sterowane będzie z poziomu wyłączników ściennych ujętych w projekcie elektrycznym.

b) Branża wentylacji i klimatyzacji

Przy prowadzeniu kanałów wentylacyjnych w przestrzeni sufitowej pomieszczeń oraz ścian należy uwzględnić lokalizację elementów konstrukcyjnych i montażowych (projektory, ekrany).

Powierzchnia projekcyjna wrażliwa jest na silniejszy nadmuch powietrza (działa jak żagiel), które może powodować falowanie ekranu lub odginanie go od pionowej płaszczyzny.

W związku z tym w systemie wentylacji i klimatyzacji należy uwzględnić rozmieszczenie ekranów i tak dostosować lokalizację urządzeń wentylacyjnych, aby uniknąć bezpośredniego nadmuchu na ekrany.

8.4 Wykaz urządzeń

a) Sala konferencyjna 2.15

L.p.	Nazwa urządzenia	Oznaczenie rysunkowe	Ilość
1	Projektor WUXGA (1920x1200), 5000lumenów	PROJ	1
2	Ekran elektryczny 240x150	EKR	1
3	Przełącznik HDMI 4:1 z deembderem	SW.HDMI	1
4	Uchwyt do projektora	-	1

5	Przylącze stołowe	PST1-PST8	8
6	Procesor DSP	DSP	1
7	Mikrofon bezprzewodowy do ręki	MIKR.x	2
8	Statyw mikrofonowy stołowy	-	2
9	Głośnik sufitowy	GS1-GS10	10
10	Wzmacniacz 100V	AMP 100V	1
11	Jednostka centralna systemu AV	J.CENTR	1
12	Panel dotykowy, bezprzewodowy	-	1
13	Oprogramowanie sterujące	-	1
14	Moduł sterujący do rozdzielni	-	2
15	Router bezprzewodowy	ROUTER	1
16	Szafa rackowa wyposażeniem	RACKAV	1
17	Okablowanie ruchome		1
18	Okablowanie stałe	-	1

8.5 Specyfikacja techniczna urządzeń

a) Sala konferencyjna 2.15

L.p.	Urządzenie	Ilość (szt.)	Opis parametrów
1.	Projektor WUXGA (1920x1200), 5000lumenów	1	<ul style="list-style-type: none"> Rozdzielczość natywna: co najmniej WUXGA 1920x1200 Technologia: 3LCD Jasność: co najmniej 5000 lumenów Współczynnik kontrastu(pełna biel/pełna czerń): co najmniej 500 000:1 Źródło światła: dioda laserowa Lens Shift: Funkcja lens shift w pionie: co najmniej od -20% do +55%, w poziomie: co najmniej +/-10%; Wejścia: co najmniej VGA, 2 x HDMI, RS232, HDBaseT (RJ-45), Video Obiektyw standardowy o współczynniku projekcji co najmniej od 1.29:1 do 1.87:1 Waga: nie większa niż 9kg
2.	Ekran elektryczny 240x150	1	<ul style="list-style-type: none"> Szerokość robocza powierzchni projekcyjnej: 240cm Silnik elektryczny o mocy 230W z 5 letnią gwarancją Aluminiowa obudowa w kolorze białym do zabudowy w suficie podwieszanym Funkcja automatycznego zatrzymywania zwijania/rozwijania powierzchni Format obrazu 16:10 Tylni wysuw materiału Powierzchnia projekcyjna do projekcji przedniej o parametrach: <ul style="list-style-type: none"> Wzmocnienie:1.2 Kąt widzenia: co najmniej 150 stopni Grubość materiału: 0.41mm

3.	Przełącznik HDMI 4:1 z deembederem	1	<ul style="list-style-type: none"> • Przełączanie: 4 wejścia HDMI do 1 wyjścia HDMI. • Obsługiwane rozdzielczości: SD, HD i VESA • Obsługa UHD/4K (4096x2160) dla 4:4:4 • Transmisja sygnałów 3D Ready: kompatybilny z stereoskopowymi formatami sygnału 3D • Obsługa EDID z wewnętrzną biblioteką • Kontrola: Przycisk na obudowie, czujnik IR, port IR, RS-232, TCP/IP • Wyjście analogowe audio: symetryczne, niesymetryczne • Wyjście cyfrowe audio, koaksjalne
4.	Uchwyt do projektora	1	<ul style="list-style-type: none"> • Uchwyt kompatybilny z projektorem z punktu 1 • Dopuszczalne obciążenie dopasowane do odpowiedniego projektora • Możliwość regulacji obrotu, kąta pochylenia
5.	Przyłącze stołowe	4	<ul style="list-style-type: none"> • Przyłącze stołowe • Modułowa konstrukcja pozwalająca na wymianę złącz • Uchylna kłapa • Złącza: 2xHDMI, 2x230V
6.	Procesor DSP	1	<ul style="list-style-type: none"> • Co najmniej 8 wejść audio • Co najmniej 4 wejść mikrofonowo/liniowych • Co najmniej 4 wejść RCA • Co najmniej 6 wyjść • Co najmniej 4 wyjścia liniowe • Co najmniej 4 pasmowy korektor parametryczny • Automatyczna regulacja wzmocnienia (AGC) • Filtr antysprężeniowy: co najmniej 12 pasmowy • Opóźnienie: co najmniej 100ms • Latencja: co najwyżej 2.4ms • Obsługa za pomocą dedykowanych sterowników lub urządzeń z systemem iOS, Android, Windows • Pasmo przenoszenia: co najmniej 20Hz – 20kHz (+/- 0.5dB) • Dynamika: co najmniej 106dB • Wyjście słuchawkowe • Złącze USB do konfiguracji
7.	Mikrofon bezprzewodowy do ręki	2	<ul style="list-style-type: none"> • Zakres częstotliwości pracy UHF: co najmniej 470 – 694 MHz w wybranych pasmach o szerokości do maksymalnie 72MHz • Typ modulacji radiowej: specjalistyczny, sygnał cyfrowy • Zakres dynamiki: co najmniej 120 dB (A) • Pasmo przenoszenia dźwięku toru nadajnika, zniekształcenia harmoniczne: co najmniej 20Hz-20kHz (+/-1dB), <0,1%THD • Pasmo przenoszenia przetwornika nadajnika: minimum 50Hz-15kHz. specjalnie kształtowana charakterystyka dla zastosowań wokalnych i mowy • Charakterystyka kierunkowa kapsuły/typ: kardiodalna/dynamiczna • Szyfrowanie sygnału: co najmniej 256 bitowe, certyfikowany standard AES • Moc promieniowana w.cz.: przełączana 1mW i 10mW • Liczba przełączanych częstotliwości nośnych w paśmie pracy zestawu ≥2400 • Zasięg pracy nadajnika: minimum 100m w optymalnych warunkach

			<ul style="list-style-type: none"> • Zakres regulacji czułości wejścia: co najmniej 60dB na odbiorniku • Typ akumulatora: dedykowany, wymienny, w technologii litowej (bez efektu pamięciowego) • Wskaźnik czasu pracy nadajnika: podawany na wyświetlaczu w godzinach i minutach (z dokładnością do 15 minut) • Minimalny czas pracy na akumulatorze: ≥ 10 godz • Minimalny czas pracy na baterii typu AA: ≥ 9 godz, 2x bateria AA/Alkaliczna • Obudowa: metalowa
8.	Statyw mikrofonowy stołowy	2	<ul style="list-style-type: none"> • Statyw mikrofonowy stołowy • Regulacja długości ramienia • Regulacja pochylenia ramienia • Podstawa żeliwna
9.	Głośnik sufitowy	6	<ul style="list-style-type: none"> • Co najmniej 1 przetwornik o średnicy 5.25" • Pasmo przenoszenia: co najmniej od 75Hz do 18kHz (+/- 3dB) • Pasmo przenoszenia: co najmniej od 60Hz do 20kHz (- 10dB) • Dyspersja znamionowa: co najmniej 160° • Moc znamionowa: co najmniej 100W • Odczepy transformatora: co najmniej 100W, 50W, 25W • Maksymalny SPL: co najmniej 105dB (111dB szczytowo) • Zamknięta tylna obudowa głośnika
10.	Wzmacniacz 100V	1	<ul style="list-style-type: none"> • Wzmacniacz 100V • Moc: co najmniej 1 x 90W/100V • Pasmo przenoszenia: co najmniej 60Hz – 20kHz (+0dB/- 3dB dla 1W) • THD+N: co najwyżej 1% przy pełnej mocy znamionowej • Dynamika: co najmniej 88dB • Przesłuchy, separacja kanałów: co najwyżej -60dBV • Impedancja wejściowa: co najmniej 20kOhm • 1 wejście liniowe niesymetryczne RCA, stereo • Wysokość: 1U • Szerokość: co najwyżej 215mm
11.	Jednostka centralna systemu sterowania	1	<ul style="list-style-type: none"> • Konstrukcja bazująca na procesorze ARM • Praca w sieci Ethernet IP • Pamięć stała przeznaczona dla aplikacji użytkownika • Pamięć wewnętrzna RAM 64MB • Wewnętrzny zegar • Kompatybilność z oprogramowaniem XPL2 • Pobieranie kodów IR • Złącza sterujące: • Co najmniej 3 x dwukierunkowe szeregowo RS-232/485 • Co najmniej 8 x uniwersalne: wejście cyfrowe, wejście napięciowe, wejście rezystancyjne, wyjście cyfrowe, wyjście IR, wyjście szeregowo • Wskaźniki na przednim panelu dla każdego portu sterującego • Zasilanie 24V • Możliwy montaż rackowy (dodatkowe akcesoria)
12.	Panel dotykowy,	1	<ul style="list-style-type: none"> • Rozdzielczość natywna panelu : co najmniej 1920 x 1080

	beprzewodowy		<ul style="list-style-type: none"> CPU: co najmniej 4 rdzeniowy 1,8 GHz Przekątna: co najmniej 10" Pamięć RAM: co najmniej 2GB DDR2 Pamięć wewnętrzna: co najmniej 16GB Obsługa kart pamięci microSD o pojemności 64 GB Łączność WiFi 802.11 b/g/n System operacyjny umożliwiający współpracę z jednostką centralną systemu sterowania
13.	Oprogramowanie sterujące	1	<ul style="list-style-type: none"> Aplikacja umieszczona w pamięci jednostki centralnej Możliwość uruchomienia na dowolnym urządzeniu mobilnym (IOS/Windows/Android) Brak potrzeby rejestracji oprogramowania (licencji) na nowym urządzeniu. Licencja przyporządkowana do jednostki centralnej Jedno środowisko (jeden program) do oprogramowania jednostek centralnych, paneli dotykowych i aplikacji na urządzenia mobilne. Ten sam język oprogramowania dla wymienionych elementów sterujących
14.	Moduł sterujący do rozdzielni	2	<ul style="list-style-type: none"> Co najmniej 8 przełączników o obciążalności maksymalnej 10A (obciążenie rezystancyjne) Co najmniej 8 wejść dla zewnętrznych przełączników (np. przyciski ściennie) Sterowanie przez RS-485 Przyciski do testowania na panelu przednim Wskaźniki zasilania na poszczególnych kanałach Przeznaczony do montażu w rozdzielni
15.	Router bezprzewodowy	1	<ul style="list-style-type: none"> Kompatybilność z 802.11b/g/n Co najmniej 4 porty LAN
16.	Szafa rackowa AV	1	<ul style="list-style-type: none"> Wysokość: co najmniej 15U
17.	Okablowanie ruchome	1	<ul style="list-style-type: none"> Okablowanie ruchome niezbędne do uruchomienia systemu AV

8.6 Wykaz linii

Uwagi:

1. Okablowanie prowadzić:
 - a. w ścianach pomieszczeń oraz na stropie w twardych rurach PCV podtynkowo oraz natynkowo oraz w bruzdach pod okładzinami ściennymi;
 - b. w podłodze Sali do przyłączy w podłodze w rurach sztywnych PCV lub karbowanych peszel,
 - c. dla głównych ciągów oraz przewodów wizyjnych stosować przekroje rur min. 37-48 mm; odejścia prowadzić w rurach o przekrojach 18-28 mm zgodnie z obowiązującymi zasadami i normami.
2. Przy szafach rackowych zostawić rezerwę min. 150 cm kabla od miejsca wypustu.
3. Przy rozdzielni zostawić rezerwę 200 cm kabla.
4. Przy przyłączach stołowych zostawić rezerwę 100 cm.

5. Linie zasilające należy prowadzić w oddzielnych rurkach niż główne ciągi tras a/v.
6. Przed przystąpieniem do realizacji zadania należy uzgodnić dokładny sposób prowadzenia przewodów z inspektorem nadzoru oraz wykonawcami branż pokrewnych

a) Sala konferencyjna 2.27

L.p.	Nazwa	Skąd	Dokąd	Typ przewodu
1	LHDMIPST1	Szafa rackowa RACK AV	Przylącze stołowe PST1	HDMI
2	LHDMIPST2	Szafa rackowa RACK AV	Przylącze stołowe PST2	HDMI
3	LHDMIPST3	Szafa rackowa RACK AV	Przylącze stołowe PST3	HDMI
4	LHDMIPST4	Szafa rackowa RACK AV	Przylącze stołowe PST4	HDMI
5	LHDMIPST5	Szafa rackowa RACK AV	Przylącze stołowe PST1	HDMI
6	LHDMIPST6	Szafa rackowa RACK AV	Przylącze stołowe PST2	HDMI
7	LHDMIPST7	Szafa rackowa RACK AV	Przylącze stołowe PST3	HDMI
8	LHDMIPST8	Szafa rackowa RACK AV	Przylącze stołowe PST4	HDMI
9	LHDMIPROJ	Szafa rackowa RACK AV	Projektor	HDMI
10	LRS PROJ	Szafa rackowa RACK AV	Projektor	Mikrofonowy, CAT6 ekranowany
11	LRE	Szafa rackowa RACK AV	Rozdzielnia	Mikrofonowy, CAT6 ekranowany
12	LGZGS1	Szafa rackowa RACK AV	Głośnik sufitowy GS1	N2XH-j 2x1
13	LGZGS2	Głośnik sufitowy GS1	Głośnik sufitowy GS2	N2XH-j 2x1
14	LGZGS3	Głośnik sufitowy GS2	Głośnik sufitowy GS3	N2XH-j 2x1
15	LGZGS4	Głośnik sufitowy GS3	Głośnik sufitowy GS4	N2XH-j 2x1
16	LGZGS5	Głośnik sufitowy GS4	Głośnik sufitowy GS5	N2XH-j 2x1
17	LGZGS6	Głośnik sufitowy GS5	Głośnik sufitowy GS6	N2XH-j 2x1
18	LGZGS3	Głośnik sufitowy GS2	Głośnik sufitowy GS3	N2XH-j 2x1
19	LGZGS4	Głośnik sufitowy GS3	Głośnik sufitowy GS4	N2XH-j 2x1
20	LGZGS5	Głośnik sufitowy GS4	Głośnik sufitowy GS5	N2XH-j 2x1
21	LGZGS6	Głośnik sufitowy GS5	Głośnik sufitowy GS6	N2XH-j 2x1

7. INSTALACJA TV/SAT

Projektuje się zamontowanie dwóch gniazd TV/SAT w pomieszczeniach 1.12. Instalację należy wykonać w oparciu o rzuty oraz schemat instalacji przedstawiony w części rysunkowej.

- przekucia przez stropy i ściany zabezpieczyć gipsem lub rurkami elektroinstalacyjnymi PCV
- przejścia kabli i przewodów przez ściany należy uszczelnić systemowo do klasy odporności ogniowej nie mniejszej niż ta przegroda
- przewody antenowe układać w trasach kablowych obwodów niskoprądowych pod podłogą techniczną

- gniazda RTV zamontować maksymalnie na wysokości 0,3m poniżej sufitu
- podłączenia do urządzeń wykonać zgodnie z DTR
- montaż instalacji wykonać należy zgodnie z projektem wykonawczym oraz obowiązującymi normami

Odstępstwa od projektu uzgodnione z projektantem należy nanieść w dokumentacji powykonawczej.

8. SYSTEM KOLEJKOWY

9.1 Opis systemu

Platforma graficzna jest to najwyższej klasy w pełni skalowalne rozwiązanie przystosowane do szybkiej i łatwej adaptacji i konfiguracji. Platforma dedykowana jest dla wdrożeń z jednym oddziałem jak i obejmujących sieć oddziałów i jeden centralny serwer aplikacji. Rozwiązanie oparte jest na aplikacji działającej wyłącznie w środowisku webowym. Wszelkie prace związane z konfiguracją, zarządzaniem i eksploatacją systemu realizowane są za pośrednictwem przeglądarki internetowej. Ogranicza to koszty związane z wdrożeniem i utrzymaniem systemu oraz pozwala na pracę w systemie w dowolnym miejscu w dowolnym czasie.

Korzyści wynikające z posiadania systemu to:

- Centralna administracja: niższe koszty operacyjne (utrzymanie w ruchu, konserwacja)
- Komunikacja poprzez LAN/WAN
- Serwer systemu może być zlokalizowany w jednym miejscu z innymi serwerami
- Możliwość wykorzystania serwerów wirtualnych i architektury 64-bitowej
- Zapis wszystkich danych w jednym miejscu (centralna baza danych operacyjnych statystycznych systemu)
- Uproszczona i ujednolicona standaryzacja procedur i sposobu obsługi klientów całej sieci oddziałów, jednolite reguły biznesowe
- Prosty benchmark oddziałów (osiągi, wyniki, identyfikacja najlepszych praktyk)
- Prosta adaptacja - każdy oddział może funkcjonować z uwzględnieniem lokalnych potrzeb i wymagań
- Możliwość grupowania oddziałów, np. ze względu na wielkość, czy lokalizację
- Logowanie do systemu za pomocą LDAP
- Centralny system licencjonowania

9.2 Organizacja systemu

System będzie obejmował:

- Sala obsługi klienta – 5 stanowisk

System będzie składał się z:

- Automatu biletowego

- Monitorów podwieszanych w Sali oczekiwań
- Głośników sufitowych
- Terminali stanowiskowych
- Interfejsu głosowego
- Interfejsu SAT
- Wzmacniacza Audio
- Komputera sterującego

Do zarządzania systemem, niezbędny jest serwer o minimalnych wymaganiach takich jak:

- 8 CPU cores ($\geq 2.6\text{GHz}$)
- 12 GB RAM
- 500 GB dysk

9.3 Elementy systemu

a) Automat biletowy

Automat biletowy stosowany jest jako kiosk biletowy w systemach obsługi klientów. Jego podstawową funkcją jest przedstawienie klientom dostępnych grup usług i wydanie biletu do wybranego przez klienta rodzaju obsługi. Posiada on 17" monitor dotykowy z drukarką biletów oraz wbudowany komputer pracujący pod kontrolą systemu operacyjnego Linux. Monitor dotykowy LCD umożliwia skuteczną informację (również reklamę produktów) poprzez projektowanie czytelnych i estetycznych plansz wyświetlanych na ekranie. Wbudowana drukarka biletów umożliwia drukowanie informacji w dowolnym języku. Może on być umieszczony na podstawie podłogowej, ladzie/stole lub przymocowany do ściany.

Funkcjonalność:

- Możliwość pracy w trybie rozproszonym.
- Oparty na Linuxie.
- 17-calowy, kolorowy monitor dotykowy LCD z pojemnościową nakładką dotykową.
- Komunikacja Ethernet.
- Całkowicie płaska górna powierzchnia szkła.
- Wbudowana przeglądarka web.
- Wsparcie dla dowolnych wersji językowych.
- Wbudowana kamera i dwa głośniki stereo.
- Aktywny iBeacon.
- Wykonanie w aluminium i czarnym szkłe.
- Możliwość przymocowania do ściany, postawienia na ladzie/stole lub podłodze.
- Możliwość customizacji poprzez umieszczenie znaków (logo) lub tekstów korporacyjnych.
- Opcjonalnie czytnik kart magnetycznych do identyfikacji klientów.
- Opcjonalnie zestaw połączenia sufitowego do przeprowadzenia kabli z sufitu.

Waga: 18,0 kg

Materiał: obudowa Aluminium i szkło

Druk: Drukarka termiczna

Szybkość wydruku: 140 mm/s,

Rodzaj papieru: Termiczny

Monitor: 17", 16.7 milionów kolorów
Rozdzielczość: 1280 X 1024 pikseli
Współczynnik kontrastu: 800.1
Jasność: 350 cd/m²
Kąt widzenia: z lewej strony, prawej strony, z góry, z dołu: 80 stopni
Dźwięk Formaty obsługiwane: .opus; .weba; .ogg; wav.
Nakładka dotykowa: Pojemnościowa
Zasilanie zewnętrzne: Wejście: 100-240 V AC, 50-60 Hz,
Wyjście: 24 V DC, 5 A
Zużycie energii Czuwanie: średnio 45 W,
Praca: max 125 W
Temperatura Praca: 10-40oC **Przechowywanie:** 0-40oC
Wilgotność względna: Praca: 15-75%, **Przechowywanie:** 10-90%
Szybkość transmisji sieci Obsługiwane: 10/100 Mbit/s Ethernet, minimum: 10 Mbit/s
Złącza/ kable: RJ45 – CAT5 – FTP / S-FTP lub wyższy elastyczny, odporny na zginanie
Przewidywana żywotność głowicy drukującej: Wydruk ponad 1,65 milionów standardowych biletów (60 mm) przy średnim stopniu zadrukowania 12,5%
Certyfikaty: CE, RoHS2, WEEE

9.4 Wyświetlacze stanowiskowe

Nad stanowiskami zamontować wyświetlacze diodowe czteroznakowe. W chwili przywołania, numer klienta na wyświetlaczu będzie mrugał przez pewien czas w celu ułatwienia dojścia klientowi do właściwego stanowiska/gabinetu.

9.5 Wyświetlacze główne – monitory.

Wyświetlacze główne służą przywoływaniu pacjentów, poprzez wskazanie numeru pacjenta oraz numeru wzywającego stanowiska/gabinetu. Jako wyświetlacze główne proponujemy zastosować monitory 43", które zostaną zamontowane w strefach oczekiwania. Każdy z monitorów będzie posiadał komputer typ player.

9.6 Głośniki

Moc znamionowa: 10W
Czułość (1m, 1W): 92bD
Pasmo przenoszenia: 150-15kHz
Wymiary (mm): 260x185x120
Materiał: HIPS
Waga (kg): 1,3

9.7 Interfejs SAT

Interfejs umożliwia łączenie urządzeń w systemie. Dzięki gniazdom modułarnym

można w łatwy sposób podłączyć i odłączyć większość urządzeń. Nie wymaga wprowadzania ustawień, dodatkowych przełączników i zworek.

Funkcjonalność:

- Cztery gniazda modularne do podłączenia urządzeń wymagających zasilania
- Dwa gniazda modularne bez pinowych gniazd zasilania, umożliwia to podłączenie automatów biletowych oraz spinanie kilku interfejsów razem
- Może być wyposażony w kostkę umożliwiającą podłączenie kabli bez złącza modułowego
- Trzy diodowy wskaźnik obecności zasilania i sygnału informacyjnego
- Zabezpieczenie przed przeciążeniem

9.8 Interfejs głosowy

Funkcjonalność

- Zapowiedzi w wysokiej jakości dźwięku,
- Możliwość przechowywania do 6 godzin dźwięku stereo w jakości CD,
- Możliwość łatwej zmiany tekstów przy użyciu pendrive USB,
- Obsługa najpopularniejszych formatów plików audio,
- Możliwość generowania zapowiedzi w różnych językach,
- Sprzętowa i programowa regulacja głośności,
- Możliwość odtwarzania dźwięku w dowolnym miejscu,
- Wbudowany wzmacniacz audio (do małych instalacji),
- Dwa kanały mogą pracować niezależnie lub w trybie stereo,
- Kostka do podłączenia głośników,
- Wyjście liniowe audio,
- Gniazdo Ethernet / TCP/IP, 1
- Możliwość zastąpienia standardowego Ding-dong przez melodyjki lub dzingle.

9.9 Wzmacniacz audio

Moc max: 2 x 50WMAX

Stereo: 4Ω 2 x 25WRMS

Stereo: 8Ω 2 x 20WRMS

Wejścia: 175mV/8kΩ (linia) 2.5mV/3.5kΩ (mikr.)

Pasmo przenoszenia: 20-20 000Hz

Stosunek S/N: 62dB

Echo cyfrowe: 200 msek.

Korektor niskie: ±10dB wysokie: ±10dB

Zasilanie: 230V̇ /50Hz/150VA

Dopuszcz. temp. Otoczenia: 0-40 °C

Wymiary: 432x45x275mm

Waga: 4kg

Połączenia linia: RCA L/P mikr.: gniazdo 6.3mm rec.:

RCA L/P głośniki: gniazda sprężynkowe

9.10 Komputer sterujący

Komputer dedykowany do obsługi systemu dostarczany w komplecie z resztą urządzeń.

9. SPIS RYSUNKÓW

En/1	RZUT PARTERU - INSTALACJE SŁABOPRĄDOWE
En/2	RZUT I PIĘTRA - INSTALACJE SŁABOPRĄDOWE
En/3	RZUT II PIĘTRA - INSTALACJE SŁABOPRĄDOWE

Sprawdzający:
inż. Jerzy Jagas

.....
upr. Bud. ŁOD/IE/1530/02 w spec instalacyjno-
inżynieryjnej w zakresie sieci elektrycznych./bez
ograniczeń/

Sprawdzający:
mgr inż. Jacek Frydrysiak

.....
upr. Bud. 617/94/WŁ w spec instalacyjno-
inżynieryjnej w zakresie sieci elektrycznych./bez
ograniczeń/