INDUSTRIA PROJECT Sp. z o.o.
80-298 Gdańsk, ul. Azymutalna 9
T. +48 (0)58 554 81 96, F. +48 (0)58 551 18 57
biuro@ibg.gda.pl, www.ibg.gda.pl

INDUSTRIA PROJECT

Inwestor:	**„Szpitale Wielkopolski" Sp. z o. o.** ul. Lutycka 34, 60-415 Poznań
Temat:	**BUDOWA WIELKOPOLSKIEGO CENTRUM ZDROWIA DZIECKA (SZPITALA PEDIATRYCZNEGO) WRAZ Z JEGO WYPOSAŻENIEM**
Adres:	ul. Adama Wrzoska, 60-663 Poznań, dz. nr ewid. 2/29, 2/17, 2/22, ark. 27, obręb Golęcin, jedn. ewid. Poznań
Kategoria obiektu:	**XI, XXII, XXIV, XXV, XXVI, XXIX, XXX**
Stadium:	PROJEKT WYKONAWCZY
Nr projektu:	**IBG-P/159/16**
Tom:	**II - OBIEKTY KUBATUROWE**
Część:	XIII - BRANŻA TELEKOMUNIKACYJNA
Projektant:	mgr inż. Jerzy Grubiak upr. nr POM/0175/PWOT/08 w specjalności telekomunikacyjnej bez ograniczeń
Opracował:	mgr inż. Mirosław Arentowicz mgr inż. Joanna Sikora inż. Łukasz Kowalski
Kierownik Projektu	dr inż. Włodzimierz Werochowski upr. nr POM/0093/POOK/06 w specjalności konstrukcyjno-budowlanej do projektowania bez ograniczeń
Sprawdzający:	mgr inż. Radosław Markiewicz upr. nr POM/0002/POOT/09 w specjalności telekomunikacyjnej bez ograniczeń

Gdańsk 12.2017

(Stronica pusta)

1 ZAWARTOŚĆ PROJEKTU

1.1 Spis kompletnej, wielobranżowej dokumentacji projektowej

SPIS ZAWARTOŚCI PROJEKTU WYKONAWCZEGO:

*szczegółowe spisy treści w poszczególnych częściach

Tom I – PROJEKT ZAGOSPODAROWANIA TERENU

CZĘŚĆ I	DOKUMENTY FORMALNE
CZĘŚĆ II	PROJEKT ZAGOSPODAROWANIA TERENU Z ELEMENTAMI MAŁEJ ARCHITEKTURY
CZĘŚĆ III	PROJEKT ZIELENI
CZĘŚĆ IV	PROJEKT DROGOWY - UKŁAD DROGOWY
CZĘŚĆ V	PROJEKT TYMCZASOWEGO DOJAZDU DO PLACU BUDOWY
CZĘŚĆ VI	PROJEKT DOCELOWEJ ORGANIZACJI RUCHU
CZĘŚĆ VII	PROJEKT KONSTRUKCYJNY
CZĘŚĆ VIII	PROJEKT PRZEBUDOWY SIECI CIEPŁOWNICZEJ
CZĘŚĆ IX	PROJEKT SIECI GAZOWEJ
CZĘŚĆ X	PROJEKT PRZEBUDOWY WODOCIĄGU DN200 I INSTALACJI TLENU
CZĘŚĆ XI	PROJEKT ZEWNĘTRZNYCH INSTALACJI SANITARNYCH
CZĘŚĆ XII	PROJEKT ELEKTRYCZNY
CZĘŚĆ XIII	PROJEKT ELEKTRYCZNY - ZASILANIE PLACU BUDOWY
CZĘŚĆ XIV	PROJEKT TELEKOMUNIKACYJNY

Tom II – OBIEKTY KUBATUROWE

Część I	ARCHITEKTURA
Część II	SYSTEM ODDYMIANIA KLATEK SCHODOWYCH i SZYBÓW WINDOWYCH Z NAWIEWEM MECHANICZNYM
Część III	TECHNOLOGIA MEDYCZNA Z LOGISTYKA SZPITALNĄ
Część IV	PROJEKT WNĘTRZ WRAZ Z PROJEKTEM WYPOSAŻENIA
Część V	SYSTEM IDENTYFIKACJI WIZUALNEJ
Część VI	PROJEKT OCHRONY RADIOLOGICZNEJ
Część VII	PROJEKT KONSTRUKCYJNY
Część VIII	PROJEKT INSTALACJI WOD-KAN
Część IX	PROJEKT INSTALACJI C.O. , C.T.
Część X	PROJEKT INSTALACJI WENTYLACJI MECHANICZNEJ I KLIMATYZACJI ORAZ WODY LODOWEJ
Część XI	PROJEKT WĘZŁA CIEPLNEGO
Część XII	PROJEKT ELEKTRYCZNY
Część XIII	PROJEKT TELEKOMUNIKACYJNY
Część XIV	PROJEKT BMS
Część XV	PROJEKT INSTALACJI GAZÓW MEDYCZNYCH
Część XVI	PROJEKT INSTALACJI POCZTY PNEUMATYCZNEJ
Część XVII	PROJEKT INSTALACJI SYSTEMU GASZENIA GAZEM
Część XVIII	URZĄDZENIE POMOCNICZE, TZW. TLENOWNIA
Część XIX	INFORMACJA DO PLANU BiOZ

1.2 Spis zawartości tomu II części XIII – branża telekomunikacyjna

1 ZAWARTOŚĆ PROJEKTU ... 3
1.1 Spis kompletnej, wielobranżowej dokumentacji projektowej ... 3
1.2 Spis zawartości tomu II części XIII – branża telekomunikacyjna ... 4
1.3 Spis części rysunkowej ... 5
2 DOKUMENTY POWIĄZANE ... 9
2.1 Podstawa opracowania ... 9
3 DANE OGÓLNE ... 10
3.1 Cel opracowania ... 10
3.2 Lokalizacja inwestycji ... 10
4 STAN PROJEKTOWANY ... 10
4.1.1 System Sygnalizacji Pożaru ... 10
4.1.2 Dźwiękowy System Ostrzegawczy ... 22
4.1.3 Instalacja sieci strukturalnej ... 34
4.1.3.1 Opis części aktywnej ... 34
4.1.3.2 Opis systemu telefonii IP ... 104
4.1.3.3 Opis części pasywnej ... 134
4.1.4 System Kontroli Dostępu ... 159
4.1.5 System Sygnalizacji Włamania i Napadu (SSWiN) ... 164
4.1.6 System Wideointerkomowy ... 167
4.1.7 System CCTV ... 176
4.1.8 System bezpieczeństwa SMS ... 189
4.1.9 Instalacja przyzywowa ... 195
4.1.10 System bezprzewodowej łączności głosowej dla personelu - DECT ... 205
4.1.11 System Wykrywania Gazów ... 207
4.1.12 Instalacja RTV ... 212
4.1.13 Instalacja audio-wizualna sal konferencyjnych ... 214
4.1.14 Instalacja audio-wizualna dziedzińca ... 224
4.1.15 System kolejkowy ... 241
4.1.16 Szpitalny system informatyczny ... 250
4.1.17 Integracja sal operacyjnych i endoskopowych ... 250
4.1.18 Inne systemy ... 268
4.1.19 Trasy kablowe ... 269
5 UWAGI ... 269
6 Klauzula dopuszczalności stosowania zamienników ... 271

7 Załączniki 271
7.1 Załącznik 1 – schemat połączeń ramach poszczególnych punktów dystrybucyjnych272
7.2 Załącznik 2 – planowane pokrycie siecią bezprzewodową na poszczególnych piętrach szpitala 273
7.3 Załącznik 3 – zestawienie głośników DSO 274
7.4 Załącznik 4 – lista kablowa: system integracji sal operacyjnych 275
7.5 Załącznik 5 – lista kablowa: system integracji sal endoskopowych 276
7.6 Załącznik 6 – zestawienie materiałów systemu sygnalizacji pożaru SSP 277
7.7 Załącznik 7 – zestawienie materiałów dźwiękowego systemu ostrzegawczego DSO278
7.8 Załącznik 8 – zestawienie sprzętu aktywnego LAN 279
7.9 Załącznik 9 – zestawienie elementów telefonii IP 280
7.10 Załącznik 10 – zestawienie elementów pasywnych sieci strukturalnej 281
7.11 Załącznik 11 – zestawienie elementów systemu kontroli dostępu skd 282
7.12 Załącznik 12 – zestawienie elementów systemu sygnalizacji włamania i napadu sswin 283
7.13 Załącznik 13 – zestawienie elementów systemu wideointerkomów 284
7.14 Załącznik 14 – zestawienie elementów systemu CCTV 285
7.15 Załącznik 15 – zestawienie elementów systemu bezpieczeństwa SMS 286
7.16 Załącznik 16 – zestawienie elementów systemu przyzywowego 287
7.17 Załącznik 17 – zestawienie elementów telefonii DECT 288
7.18 Załącznik 18 – zestawienie elementów systemu wykrywania gazów SWG 289
7.19 Załącznik 19 – zestawienie elementów instalacji RTV 290
7.20 Załącznik 20 – zestawienie elementów dla systemów AV 291
7.21 Załącznik 21 – zestawienie elementów systemu kolejkowego 292
7.22 Załącznik 22 – zestawienie elementów systemu integracji 293
7.23 Załącznik 23 – zestawienie elementów systemu tras kablowych 294
7.24 Załącznik 24 – zestawienie elementów systemu rejestracji czasu pracy RCP 295
8 Część rysunkowa 296

1.3 Spis części rysunkowej

L.p.	Nr rysunku	Tytuł	rewizja	skala
1.	IP159_PW_DR_IIT.61001	Koryta teletechniczne - poziom (B01)	C	1:100
2.	IP159_PW_DR_IIT.61002	Koryta teletechniczne - poziom (P00)	C	1:100
3.	IP159_PW_DR_IIT.61003	Koryta teletechniczne - poziom (P01)	C	1:100

L.p.	Nr rysunku	Tytuł	rewizja	skala
4.	IP159_PW_DR_IIT.61004	Koryta teletechniczne - poziom (P02)	C	1:100
5.	IP159_PW_DR_IIT.61005	Koryta teletechniczne - poziom (P03)	C	1:100
6.	IP159_PW_DR_IIT.61006	Koryta teletechniczne - poziom (P04)	C	1:100
7.	IP159_PW_DR_IIT.61007	Koryta teletechniczne - poziom (P05)	C	1:100
8.	IP159_PW_DR_IIT.61008	Koryta teletechniczne - poziom dachu	C	1:100
9.	IP159_PW_DR_IIT.62001	System Sieci Strukturalnej LAN oraz instalacja RTV - poziom (B01)	C	1:100
10.	IP159_PW_DR_IIT.62002	System Sieci Strukturalnej LAN oraz instalacja RTV - poziom (P00)	C	1:100
11.	IP159_PW_DR_IIT.62003	System Sieci Strukturalnej LAN oraz instalacja RTV - poziom (P01)	C	1:100
12.	IP159_PW_DR_IIT.62004	System Sieci Strukturalnej LAN oraz instalacja RTV - poziom (P02)	C	1:100
13.	IP159_PW_DR_IIT.62005	System Sieci Strukturalnej LAN oraz instalacja RTV - poziom (P03)	C	1:100
14.	IP159_PW_DR_IIT.62006	System Sieci Strukturalnej LAN oraz instalacja RTV - poziom (P04)	C	1:100
15.	IP159_PW_DR_IIT.62007	System Sieci Strukturalnej LAN oraz instalacja RTV - poziom (P05)	C	1:100
16.	IP159_PW_DR_IIT.62008	System Sieci Strukturalnej LAN - poziom (P06)	A	1:100
17.	IP159_PW_DR_IIT.62009	System Sieci Strukturalnej LAN - schemat ideowy	B	-
18.	IP159_PW_DR_IIT.62010	System Sieci Strukturalnej LAN - widoki szaf	C	-
19.	IP159_PW_DR_IIT.62011	Instalacja RTV - schemat blokowy	A	-
20.	IP159_PW_DR_IIT.63001	System Sygnalizacji Pożaru - poziom (B01)	D	1:100
21.	IP159_PW_DR_IIT.63002	System Sygnalizacji Pożaru - poziom (P00)	C	1:100
22.	IP159_PW_DR_IIT.63003	System Sygnalizacji Pożaru - poziom (P01)	C	1:100
23.	IP159_PW_DR_IIT.63004	System Sygnalizacji Pożaru - poziom (P02)	C	1:100
24.	IP159_PW_DR_IIT.63005	System Sygnalizacji Pożaru - poziom (P03)	C	1:100
25.	IP159_PW_DR_IIT.63006	System Sygnalizacji Pożaru - poziom (P04)	C	1:100
26.	IP159_PW_DR_IIT.63007	System Sygnalizacji Pożaru - poziom (P05)	C	1:100
27.	IP159_PW_DR_IIT.63008	System Sygnalizacji Pożaru - poziom dachu	B	1:100
28.	IP159_PW_DR_IIT.63009	System Sygnalizacji Pożaru - schemat blokowy	C	-
29.	IP159_PW_DR_IIT.63101	Dźwiękowy system ostrzegawczy DSO - poziom (B01)	C	1:100
30.	IP159_PW_DR_IIT.63102	Dźwiękowy system ostrzegawczy DSO - poziom (P00)	C	1:100
31.	IP159_PW_DR_IIT.63103	Dźwiękowy system ostrzegawczy DSO - poziom (P01)	C	1:100
32.	IP159_PW_DR_IIT.63104	Dźwiękowy system ostrzegawczy DSO - poziom (P02)	C	1:100
33.	IP159_PW_DR_IIT.63105	Dźwiękowy system ostrzegawczy DSO - poziom (P03)	C	1:100
34.	IP159_PW_DR_IIT.63106	Dźwiękowy system ostrzegawczy DSO - poziom (P04)	C	1:100
35.	IP159_PW_DR_IIT.63107	Dźwiękowy system ostrzegawczy DSO - poziom (P05)	C	1:100
36.	IP159_PW_DR_IIT.63108	Dźwiękowy system ostrzegawczy DSO - poziom dachu	B	1:100
37.	IP159_PW_DR_IIT.63109	Dźwiękowy system ostrzegawczy DSO - schemat strukturalny systemu	A	1:100
38.	IP159_PW_DR_IIT.63110	Dźwiękowy system ostrzegawczy DSO - schemat szafy DSO1	B	1:100
39.	IP159_PW_DR_IIT.63111	Dźwiękowy system ostrzegawczy DSO - schemat szafy DSO2	B	1:100
40.	IP159_PW_DR_IIT.63112	Dźwiękowy system ostrzegawczy DSO - schemat szafy DSO3	B	1:100
41.	IP159_PW_DR_IIT.63113	Dźwiękowy system ostrzegawczy DSO - schemat szafy DSO4	B	1:100
42.	IP159_PW_DR_IIT.64001	CCTV+SKD - poziom (B01)	B	1:100
43.	IP159_PW_DR_IIT.64002	CCTV+SKD - poziom (P00)	B	1:100
44.	IP159_PW_DR_IIT.64003	CCTV+SKD - poziom (P01)	B	1:100
45.	IP159_PW_DR_IIT.64004	CCTV+SKD - poziom (P02)	B	1:100
46.	IP159_PW_DR_IIT.64005	CCTV+SKD - poziom (P03)	B	1:100
47.	IP159_PW_DR_IIT.64006	CCTV+SKD - poziom (P04)	B	1:100
48.	IP159_PW_DR_IIT.64007	CCTV+SKD - poziom (P05)	B	1:100

L.p.	Nr rysunku	Tytuł	rewizja	skala
49.	IP159_PW_DR_IIT.64008	CCTV+SKD - poziom dachu	B	1:100
50.	IP159_PW_DR_IIT.64009	CCTV- schemat blokowy	B	-
51.	IP159_PW_DR_IIT.65009	System Kontroli Dostępu i łączności interkomowej - schemat blokowy	B	1:100
52.	IP159_PW_DR_IIT.65010	System Sygnalizacji Włamania i Napadu - poziom (B01)	B	1:100
53.	IP159_PW_DR_IIT.65011	System Sygnalizacji Włamania i Napadu - poziom (P05)	B	1:100
54.	IP159_PW_DR_IIT.65012	System Sygnalizacji Włamania i Napadu - schemat blokowy	B	1:100
55.	IP159_PW_DR_IIT.67001	Instalacja Systemu Kolejkowego - poziom (B01)	B	1:100
56.	IP159_PW_DR_IIT.67002	Instalacja Systemu Kolejkowego na IPP oraz ZDO - poziom (P00)	B	1:100
57.	IP159_PW_DR_IIT.67003	Instalacja Systemu Kolejkowego na SOR - poziom (P00)	B	1:100
58.	IP159_PW_DR_IIT.67004	Instalacja Systemu Kolejkowego na ZPS - poziom (P01)	B	1:100
59.	IP159_PW_DR_IIT.67005	Instalacja Systemu Kolejkowego na EDG - poziom (P02)	B	1:100
60.	IP159_PW_DR_IIT.67006	Schemat blokowy Systemu Kolejkowego	B	-
61.	IP159_PW_DR_IIT.68001	System Integracji - poziom (P02) sale operacyjne I i II	B	1:200
62.	IP159_PW_DR_IIT.68002	System Integracji - poziom (P02) sala operacyjna III	B	1:200
63.	IP159_PW_DR_IIT.68003	System Integracji - poziom (P02) sala operacyjna IV	B	1:200
64.	IP159_PW_DR_IIT.68004	System Integracji - poziom (P02) sala operacyjna V	B	1:200
65.	IP159_PW_DR_IIT.68005	System Integracji - poziom (P02) endoskopia	B	1:100
66.	IP159_PW_DR_IIT.68006	System Integracji - schemat blokowy sal operacyjnych	B	-
67.	IP159_PW_DR_IIT.68007	System Integracji - schemat blokowy endoskopii	B	-
68.	IP159_PW_DR_IIT.68008	System audio-wizualny - poziom (P02) CDK	B	1:100
69.	IP159_PW_DR_IIT.68009	System audio-wizualny - poziom (P05) administracja	B	1:100
70.	IP159_PW_DR_IIT.68010	Schemat systemu audio-wizualnego - sala 2.505	A	-
71.	IP159_PW_DR_IIT.68011	Schemat systemu audio-wizualnego: szafa AV - sala 2.505	A	-
72.	IP159_PW_DR_IIT.68012	Schemat systemu audio-wizualnego: wyposażenie rozdzielnicy - sala 2.505	A	-
73.	IP159_PW_DR_IIT.68013	Schemat systemu audio-wizualnego: widok szafy AV - sala 2.505	A	-
74.	IP159_PW_DR_IIT.68014	Schemat systemu audio-wizualnego - sala 5.011	A	-
75.	IP159_PW_DR_IIT.68015	Schemat systemu audio-wizualnego: szafa AV - sala 5.011	A	-
76.	IP159_PW_DR_IIT.68016	Schemat systemu audio-wizualnego: wyposażenie rozdzielnicy - sala 5.011	A	-
77.	IP159_PW_DR_IIT.68017	Schemat systemu audio-wizualnego: widok szafy AV - sala 5.011	A	-
78.	IP159_PW_DR_IIT.68020	System Wykrywania Gazów - strefa dostaw	B	1:100
79.	IP159_PW_DR_IIT.68021	System Wykrywania Gazów - pom. tech. IT	B	1:100
80.	IP159_PW_DR_IIT.68022	System Wykrywania Gazów - pom. UPS i baterii	B	1:100
81.	IP159_PW_DR_IIT.68023	System Wykrywania Gazów - pom. UPS/sprężarkownia	B	1:100
82.	IP159_PW_DR_IIT.68024	System Wykrywania Gazów - ciepła sień	B	1:100
83.	IP159_PW_DR_IIT.68025	System Wykrywania Gazów - rozprężalnia CO2	B	1:100
84.	IP159_PW_DR_IIT.68026	System Wykrywania Gazów - schemat blokowy	B	-
85.	IP159_PW_DR_IIT.68027	System audio-wizualny - dziedziniec	B	1:100
86.	IP159_PW_DR_IIT.68028	System audio-wizualny - dziedziniec. Schemat blokowy	A	-
87.	IP159_PW_DR_IIT.68029	System audio-wizualny. Wyposażenie rozdzielnicy - dziedziniec	A	-
88.	IP159_PW_DR_IIT.68030	System audio-wizualny - dziedziniec. Szafa AV/01	A	-
89.	IP159_PW_DR_IIT.68031	System audio-wizualny - dziedziniec. Szafa AV/02	A	-
90.	IP159_PW_DR_IIT.69001	Instalacja przyzywowa - poziom (B01)	B	1:100
91.	IP159_PW_DR_IIT.69002	Instalacja przyzywowa - poziom (P00)	B	1:100
92.	IP159_PW_DR_IIT.69003	Instalacja przyzywowa - poziom (P01)	B	1:100
93.	IP159_PW_DR_IIT.69004	Instalacja przyzywowa - poziom (P02)	B	1:100

L.p.	Nr rysunku	Tytuł	rewizja	skala
94.	IP159_PW_DR_IIT.69005	Instalacja przyzywowa - poziom (P03)	B	1:100
95.	IP159_PW_DR_IIT.69006	Instalacja przyzywowa - poziom (P04)	B	1:100
96.	IP159_PW_DR_IIT.69007	Instalacja przyzywowa - poziom (P05)	B	1:100
97.	IP159_PW_DR_IIT.69008	Instalacja przyzywowa - schemat ideowy (B01)	B	-
98.	IP159_PW_DR_IIT.69009	Instalacja przyzywowa - schemat ideowy (P00)	B	-
99.	IP159_PW_DR_IIT.69010	Instalacja przyzywowa - schemat ideowy (P01)	B	-
100.	IP159_PW_DR_IIT.69011	Instalacja przyzywowa - schemat ideowy (P02)	B	-
101.	IP159_PW_DR_IIT.69012	Instalacja przyzywowa - schemat ideowy (P03)	B	-
102.	IP159_PW_DR_IIT.69013	Instalacja przyzywowa - schemat ideowy (P04)	B	-
	IP159_PW_DR_IIT.69014	Instalacja przyzywowa - schemat ideowy (P05)	B	-

2 DOKUMENTY POWIĄZANE

2.1 Podstawa opracowania

- Umowa na wykonanie prac projektowych,
- Konsultacje i uzgodnienia z zakresu ochrony p.poż., BHP, warunków higieniczno-sanitarnych,
- Projekt budowlany wielobranżowy,
- Pozwolenie na budowę nr 1933/2017 z dnia 05.09.2017 roku, NR UA-VI-A04.6740.1760.2017,
- Aktualna mapa do celów projektowych w skali 1:500,
- Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 25 kwietnia 2012 r. w sprawie szczegółowego zakresu i formy projektu budowlanego (Dz. U. z 2012 r. poz. 462, z późniejszymi zmianami),
- Ustawa z dnia 7 lipca 1994 r. - Prawo budowlane (Dz.U. z 1994 r. Nr 89 poz. 414, z późniejszymi zmianami),
- Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 roku w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 2002 r. Nr 75, poz. 690, z późniejszymi zmianami),
- Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 roku w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (Dz. U. z 1997 r. Nr 129, poz. 844, z późniejszymi zmianami),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 07 czerwca 2010 roku w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. z 2010 r. Nr 109, poz. 719),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2009 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych (Dz. U. z 2009 r. Nr 124, poz. 1030),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 grudnia 2015 r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej (Dz.U. z 2015 r. poz. 2117),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 czerwca 2007 roku w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz. U. z 2007 r. Nr 143, poz. 1002, z późniejszymi zmianami),
- Rozporządzenie Ministra Infrastruktury z dnia 11 sierpnia 2004 roku w sprawie sposobów deklarowania zgodności wyrobów budowlanych oraz sposobu znakowania ich znakiem budowlanym (Dz. U. z 2004 r. Nr 198, poz. 2041, z późniejszymi zmianami),
- Załącznik nr 2 do rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 5 lipca 2013 (poz. 926) Objęte tekstem jednolitym (Dz. U. z 2015 r. poz. 1422), z wyjątkiem par. 2 oraz odnośnika nr 2,
- Obowiązujące normy, m.in. PN-EN 54, CEN/TS 54-32,
- Wytyczne projektowania instalacji sygnalizacji pożarowej SITP WP-02:2010,
- Program Funkcjonalno Użytkowy oraz opracowanie koncepcyjne,
- Zasady wiedzy technicznej.

3 DANE OGÓLNE

3.1 Cel opracowania

Celem opracowania jest przygotowanie wielobranżowego projektu wykonawczego dla inwestycji pn. „Budowa Wielkopolskiego Centrum Zdrowia Dziecka (szpitala pediatrycznego) wraz z jego wyposażeniem”.

3.2 Lokalizacja inwestycji

Przedmiotowa inwestycja usytuowana jest w Poznaniu przy ul. A. Wrzoska na działce nr 2/29 (ark. 27, obr. Golęcin).

4 STAN PROJEKTOWANY

4.1.1 System Sygnalizacji Pożaru

Zakres realizacji

Na potrzeby Wielkopolskiego Centrum Zdrowia Dziecka projektuje się System Sygnalizacji Pożaru. System Sygnalizacji Pożaru jest wymagany zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. Nr 109 poz. 719).

Projekt został opracowany zgodnie ze scenariuszem pożarowym. Projektuje się ochronę pełną obiektu, chronione nie będą wybrane pomieszczenia niewymagające ochrony [np. wybrane sanitariaty oraz szachty sanitarne gdzie wprowadzono eliminację efektu kominowego (na każdej kondygnacji jest przegroda)], pomieszczenia objęte systemem oddymiania z napowietrzaniem mechanicznym oraz pomieszczenia objęte Stałymi Urządzeniami Gaśniczymi. Główna centrala systemu zostanie umieszczona w pomieszczeniu ochrony na parterze przy wejściu głównym (pom. 0.819). Pozostałe centrale systemu zostaną zlokalizowane w wydzielonych pomieszczeniach technicznych na pozostałych kondygnacjach, zgodnie z częścią rysunkową.

Zadaniem Systemu Sygnalizacji Pożaru będzie:

- sygnalizowanie o źródle pożaru, wykrytym przez współpracujące czujki pożarowe oraz ręczne ostrzegacze pożarowe;
- przekazanie informacji o alarmie do ochrony
- wysterowanie Dźwiękowego Systemu Ostrzegawczego;
- wskazanie miejsca zagrożonego pożarem;
- rejestracja w pamięci oraz na drukarce ważniejszych wydarzeń (wszelkiego rodzaju alarmów);
- wysterowanie i monitorowanie przeciwpożarowych urządzeń zabezpieczających, np. klap ppoż.;
- wysterowanie drzwi pożarowych oraz drzwi przesuwnych;
- wysterowanie central wentylacyjnych;
- wysterowanie wentylacji bytowej;
- wysterowanie klimatyzacji;
- wysterowanie kurtyn powietrznych;
- wysterowanie wind na zjazd na poziom ewakuacyjny;
- zwolnienie przejść na drogach ewakuacyjnych objętych SKD;

- wysterowanie i monitorowanie systemu oddymiania;
- wysterowanie siłowni pneumatycznej;
- zadziałanie zaworów elektromagnetycznych na instalacji wodnej;
- podniesienie szlabanów na drogach pożarowych;
- wysterowanie systemów AV w tryb „mute”;
- monitorowanie Stałych Urządzeń Gaśniczych;
- monitorowanie zasilaczy pożarowych;
- automatyczne przekazywanie sygnału o alarmie II stopnia do PSP;
- wysterowanie i monitorowanie innych urządzeń wymagających współpracy z SSP.

Ze względu na niezawodność działania instalacji projektuje się pętlowy system prowadzenia linii dozorowych. Główne elementy systemu, zgodnie z obowiązującymi przepisami, powinny posiadać wymagane certyfikaty zgodności lub świadectwa dopuszczenia CNBOP.

Lokalizacje elementów systemu pokazano w części rysunkowej projektu.

Opis systemu

Z uwagi na wielkość projektowanego budynku, system oparty będzie na kilku centralach połączonych w sieć. Każda z central wyposażona będzie w dodatkowe karty, moduły, akumulatory, itd. niezbędne do uzyskania ich pełnej funkcjonalności.

Automatyczna detekcja dymu realizowana będzie głównie za pomocą punktowych optycznych czujek dymu, a w uzasadnionych przypadkach należy przewidzieć wykorzystanie detektorów zasysających oraz liniowych. W projekcie przewidziano detektory zasysające do ochrony szybów windowych oraz detektory liniowe do ochrony dziedzińca. Na potrzeby ochrony kanałów wentylacyjnych przewidziano czujki w czerpniach.

W pomieszczeniach socjalnych oraz zapleczach projektuje się zastosowanie czujek wielodetektorowych z członem termicznym.

Ręczne uruchomienie sygnału alarmu II stopnia będzie następowało poprzez ręczne ostrzegacze pożarowe ROP w koincydencji z zadziałaniem czujki. Zgodnie ze scenariuszem pożarowym samo wciśnięcie przycisku ROP nie wywołuje uruchomienia DSO.

Jako elementy sterujące należy wykorzystać adresowalne moduły pętlowe wyposażone w wyjścia przekaźnikowe typu NO/NC oraz wejścia parametryczne.

Projektowanie linii dozorowych oparto na założeniu, że maksymalna ilość elementów na pętli nie będzie przekraczać 128, co wynika bezpośrednio z wytycznych projektowych CNBOP. Instalowane na obiekcie urządzenia Systemu Sygnalizacji Pożaru muszą posiadać wymagane prawem certyfikaty lub świadectwa dopuszczenia, np. wydawane przez CNBOP.

Projekt nie przewiduje nadajnika UTA. Projektowana centrala SSP jest przystosowana do powiadomienia lokalnej jednostki Państwowej Straży Pożarnej za pośrednictwem Urządzenia Transmisji Alarmów (UTA) poprzez bezpośrednie połączenie CSP z nadajnikiem UTA. Sposób transmisji sygnałów z UTA do stacji monitoringu oraz sam nadajnik UTA dostarczy firma specjalizująca się w monitoringu i transmisji alarmów po podpisaniu stosownej umowy przez Użytkownika. Połączenie między CSP i UTA należy wykonać zgodnie z obowiązującymi przepisami i wytycznymi.

Zasilanie centrali i zasilaczy pożarowych

Centrale SSP oraz zasilacze pożarowe należy zasilić napięciem 230V AC sprzed pożarowego wyłącznika prądu i za pomocą kabla o cechach PH90 z rozdzielni odbiorów pożarowych.

Baterie central SSP oraz zasilaczy pożarowych będą składały się z akumulatorów o pojemności gwarantującej 72 godziny niezależnego działania całego systemu (linie monitorujące) oraz kolejne 30 min. niezależnego działania podczas alarmu. Dopuszcza się skrócenie tego czasu w

przypadku spełnienia zapisów normy PN-EN 54 w tym zakresie. Czas ładowania: 24 godziny dla 80% pojemności.

Pojemność akumulatorów dla centrali i zasilaczy pożarowych obliczono korzystając ze wzoru:

$$Q = k(I_{CZ} * t_{CZ} + I_A * t_A)$$

gdzie:

Q	pojemność akumulatora [Ah]
k	współczynnik bezpieczeństwa, przyjęto 1,25
I_{CZ}	prąd czuwania [A]
I_A	prąd alarmowania [A]
t_{CZ}	czas czuwania [h]
t_A	czas alarmowania [h]

Zestaw zasilacza z akumulatorami przejmie zasilanie systemu zaraz po zarejestrowaniu przerwy w dostawie prądu z sieci zasilającej. Poniżej przedstawiono obliczenia akumulatorów dla zasilaczy pożarowych:

ZASILACZ ZSP.I.1

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah

projektowany akumulator 2x12V 45 Ah

ZASILACZ ZSP.I.2

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah

projektowany akumulator 2x12V 45 Ah

ZASILACZ ZSP.I.3

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah

projektowany akumulator 2x12V 45 Ah

ZASILACZ ZSP.I.4

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah

projektowany akumulator 2x12V 45 Ah

ZASILACZ ZSP.I.5

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka liniowa	2	**50**	**100**	**50**	**100**
suma				**117**		**117**

potrzebny akumulator 10,60 Ah

projektowany akumulator 2x12V 18Ah Ah

ZASILACZ ZSP.I.6

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka liniowa	2	**50**	**100**	**50**	**100**
suma				**117**		**117**

potrzebny akumulator 10,60 Ah

projektowany akumulator 2x12V 18Ah Ah

ZASILACZ ZSP.H.1

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah
projektowany akumulator 2x12V 45 Ah

ZASILACZ ZSP.H.2

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah
projektowany akumulator 2x12V 45 Ah

ZASILACZ ZSP.I.7

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah
projektowany akumulator 2x12V 45 Ah

ZASILACZ ZSP.I.8

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah
projektowany akumulator 2x12V 45 Ah

ZASILACZ ZSP.I.9

L.p.	Urządzenie	Ilość	Ialarm[mA]	pobór w czasie alarmu [mA]	Inormal[mA]	pobór w czasie czuwania [mA]
1.	Zasilacz	1	**17**	**17**	**17**	**17**
2.	czujka zasysająca	1	**400**	**400**	**400**	**400**
suma				**417**		**417**

potrzebny akumulator 37,79 Ah
projektowany akumulator 2x12V 45 Ah

Algorytm sterowań

Dwustopniowa organizacja alarmowania

W celu eliminacji fałszywych alarmów z czujek automatycznych oraz umożliwienia służbom dozoru zneutralizowania niewielkiego zagrożenia pożarowego bez konieczności wzywania jednostki Ratowniczo-Gaśniczej Straży Pożarnej oraz zbędnej ewakuacji obiektu, przyjęto dwustopniową procedurę organizacji alarmowania. Przy tak przyjętej procedurze zagrożenie wykryte przez pojedynczą czujkę automatyczną powoduje jedynie sygnalizację alarmu pożarowego I stopnia. Bez skasowania alarmu w wyznaczonym czasie system sygnalizacji pożaru automatycznie przechodzi w alarm II stopnia. Wciśnięcie przycisku ROP nie powoduje automatycznie alarmu II stopnia – konieczne jest jednoczesne zadziałanie detektora.

Alarm I stopnia:
- Zadziałanie czujki dymowej – centralka pożarowa włącza alarm akustyczny dla obsługi, na wyświetlaczu centrali pożarowej pojawia się numer czujki i nazwa, miejsca gdzie ona się znajduje; dane mogą być wydrukowane na papierze z drukarki przy centralce pożarowej.
- Wysterowanie Dźwiękowego Systemu Ostrzegawczego na rozgłaszanie komunikatu o zagrożeniu w strefie z alarmem.
- Potwierdzenie w ciągu czasu T1 - około 30 sekund przez obsługę przyjęcia alarmu, następuje poprzez naciśnięcie przycisku „potwierdzenie”; jeżeli pracownik obsługi tego nie uczyni, włącza się alarm II stopnia.
- Sprawdzenie miejsca zdarzenia - po potwierdzeniu pracownik obsługi musi sprawdzić miejsce zdarzenia w celu wykluczenia fałszywego alarmu; ma na to czas T2 przewidziany na poziomie 240s.
- W przypadku stwierdzenia fałszywego alarmu pracownik służby ochrony wraca do centralki pożarowej w celu skasowania alarmu przed upływem wyznaczonego czasu albo powiadamia o tym drogą radiową/telefoniczną innego pracownika, który skasuje alarm.
- W przypadku potwierdzenia zagrożenia niezwłocznie nacisnąć najbliższy ręczny ostrzegacz pożarowy (przycisk pożarowy ROP).
- Powyższe czasy mogą być wydłużone zgodnie z zasadami wiedzy technicznej, po przeprowadzeniu sprawdzenia czasu na dojście do rejonu zagrożonego i powrotu, w celu ustalenia dopuszczalnego czasu zwłoki.
- Przystąpić do likwidacji zagrożenia, np. użycia gaśnicy lub hydrantów.

Czasy T1 i T2 należy zweryfikować i dostosować do realnej możliwości reakcji służb dyżurnych na etapie uruchomienia Systemu Sygnalizacji Pożaru, oraz dostosować do ewentualnych wytycznych Państwowej Straży Pożarnej na etapie odbiorów.

Alarm II stopnia:
Alarm II drugiego stopnia jest wywołany:
- przez czujkę wykrywania dymu, po ustalonym czasie na sprawdzenie pomieszczenia (miejsca zagrożonego), dla wszystkich pomieszczeń,
- po zadziałaniu ręcznego ostrzegacza pożarowego (przycisku pożarowego ROP) w koincydencji z pobudzeniem detektora.
- przez jednoczesne zadziałanie kilku czujek.

Alarm II stopnia powoduje:
- wysterowanie Dźwiękowego Systemu Ostrzegawczego na rozgłaszanie komunikatu o ewakuacji tylko w strefie z alarmem,
- wysterowanie Dźwiękowego Systemu Ostrzegawczego na rozgłaszanie komunikatu o zagrożeniu dla pozostałej części obiektu,
- przekazanie sygnału alarmowego do wykwalikowanego personelu i centrali głównej,
- zwolnienie przejść objętych kontrolą dostępu (na drogach ewakuacyjnych),
- wysterowanie przeciwpożarowych urządzeń zabezpieczających (w szczególności klap ppoż. i elementów automatyki systemu wentylacji),
- wysterowanie systemu klimatyzacji,
- wysterowanie drzwi przesuwnych oraz drzwi pożarowych,
- zjazd dźwigów osobowych na poziom ewakuacyjny,
- zatrzymanie pracy siłowni pneumatycznej,
- zamknięcie zaworów elektromagnetycznych na instalacji wodnej,
- podniesienie szlabanów na drogach pożarowych,
- wysterowanie systemów AV w tryb „mute”,
- wysterowanie innych urządzeń wymagających współpracy z SSP na wypadek pożaru (np. wyłączenie wentylacji bytowej, itp. poprzez wysterowanie styczników w rozdzielnicach elektrycznych).
- wysterowanie nadajnika UTA i automatyczne przekazanie sygnału do PSP.

Wykonanie systemu

System Sygnalizacji Pożaru stanowi niezależną wydzieloną instalację bezpieczeństwa, w związku z tym nie może być wspólny z inną siecią innej instalacji. Montaż urządzeń należy wykonać w oparciu o fabryczną dokumentację techniczno-ruchową producenta urządzeń.

Centrale powinny być zamontowane na wysokości od 1,5 do 1,8 m licząc od poziomu podłogi pomieszczenia do środkowej części centrali.

Ręczne ostrzegacze pożaru powinny być tak rozmieszczone, aby żadna osoba do najbliższego ostrzegacza nie musiała przebywać drogi dłuższej niż 30 m. Ręczne ostrzegacze należy instalować w miejscach dobrze widocznych i dostępnych, na wysokości od 1,2 m do 1,6 m w taki sposób, aby były widoczne w każdym przypadku, np. nie były przysłaniane drzwiami po ich otwarciu, itp. Czujki należy zainstalować uwzględniając rozmieszczenie elementów w poszczególnych pomieszczeniach, z uwzględnieniem wytycznych projektowania instalacji sygnalizacji pożarowej SITP WP-02:2010. Należy zwrócić uwagę, aby w miejscach gdzie jest to możliwe czujki znajdowały się w odległości większej niż 0,5m od ścian, belek stropowych, podciągów i innych przegród pionowych oraz opraw oświetleniowych oraz w odległości 1,5m od kratek wentylacyjnych nawiewnych. W przypadku pomieszczeń o gabarytach nie pozwalających na zachowanie ww. odległości należy zachować maksymalne możliwe do uzyskania odstępy między urządzeniami.

W obszarach z sufitami podwieszonymi zastosowano czujki w przestrzeni między sufitowej wyposażone we wskaźniki zadziałania. W przypadku pokoi łóżkowych należy zainstalować dodatkowy wskaźnik zadziałania nad drzwiami od strony korytarza, w celu szybszej

identyfikacji miejsca zagrożenia. Wskaźnik należy montować tak aby był widoczny dla personelu (nie we wnękach).

Przy rozmieszczeniu czujek liniowych na dziedzińcu należy zwrócić uwagę na odstępy od zadaszenia. Należy zwrócić uwagę, aby zbyt bliskie elementy zadaszania, elementów oświetlenia lub ścian nie powodowały odbić promienia i przez to obniżały czułość czujki. Wysokość poduszki powietrznej należy pomierzyć eksperymentalnie na obiekcie.

Zaleca się, aby System Sygnalizacji Pożaru był zintegrowany z systemem przyzywowym. System przyzywowy oraz telefonów medycznych personelu powinien wyświetlać wybrane komunikaty SSP (np. alarm II stopnia dla danej strefy pożarowej), co zoptymalizuje proces ewentualnego powiadamiania pacjentów o zagrożeniu i przyspieszy akcję ewakuacyjną.

Początki i końce pętli dozorowych elementów detekcyjnych (czujki oraz ROPy) należy wykonać kablem HTKSHekw 1x2x0,8 PH90. Pozostałą część tych pętli można wykonać kablem YnTKSYekw 1x2x0,8 w powłoce koloru czerwonego (ze względu na brak wymogu dotyczącego ciągłości okablowania w warunkach pożaru). Wszędzie tam, gdzie kilka kabli jest prowadzonych obok siebie, okablowanie należy wykonać kablem HTKSHekw PH90. Pętle elementów kontrolno-sterujących należy w całości wykonać okablowaniem niepalnym HTKSHekw 1x2x0,8. Należy zachować jednorodność średnicy żył kabli w pętlach. Długość i obciążalność pętli nie może przekroczyć dopuszczalnych parametrów granicznych określonych przez producenta systemu pożarowego. Należy stosować okablowanie zalecane przez producenta systemu.

Sygnalizacja pożaru zostanie wykonana z wykorzystaniem Dźwiękowego Systemu Ostrzegawczego, dlatego w obiekcie nie należy instalować innych pożarowych akustycznych urządzeń alarmowych. Na salach operacyjnych należy zainstalować sygnalizatory optyczne informujące personel o możliwym zagrożeniu.

Monitorowanie central systemu oddymiania (modułów MZS) będzie realizowane poprzez pętlowe moduły SSP.

Stan klap pożarowych musi być monitorowany przez SSP. Zamkniecie jakiejkolwiek klapy pożarowej uniemożliwi uruchomienie centrali wentylacyjnej w obwodzie której znajdowała się dana klapa. Monitorowanie stanu danej klapy ppoż. może odbywać się za pomocą jednego wejścia w danym module kontrolnym z wykorzystaniem rezystorów parametryzujących. Sterowanie alarmowym zamknięciem klap odbywać się będzie za pomocą pętlowych adresowalnych modułów kontrolno-sterujących z wykorzystaniem osobnego wyjścia dla każdej klapy.

Instalacja będzie automatycznie nadzorowana, wszelkie uszkodzenia systemu sygnalizacji pożaru muszą być bezwzględnie sygnalizowane na centralce (sygnały dźwiękowe i świetlne). Takimi sygnałami są:

- odłączenie, przerwanie lub zwarcie połączenia adresowanego,
- zwarcie doziemne.

Konstrukcje wsporcze dla instalacji zasilających urządzenia przeciwpożarowe winny spełniać kryteria zapewnienia ciągłości dostawy sygnałów lub sterowań w warunkach pożaru odpowiednio 90 lub 30 minut z zachowaniem ważnych dopuszczeń potwierdzonych certyfikatami i deklaracjami zgodności.

Konstrukcje wsporcze dla instalacji teletechnicznych zostaną wykonane według standardów obowiązujących dla pozostałych instalacji elektrycznych z zachowaniem ważnych dopuszczeń potwierdzonych certyfikatami i deklaracjami zgodności.

Przewody linii projektuje się prowadzić przy konstrukcji stropu w sposób jej nienaruszający. Pojemność przewodu linii nie powinna być większa od wartości podanej w świadectwie dopuszczenia lub przez producenta systemu. Przewody powinny być dobrane z uwzględnieniem warunków środowiskowych. Przewody powinny posiadać podwyższoną odporność na oddziaływanie płomienia - posiadać certyfikat zgodności. Każdą pętlową linie

dozorową należy dwustronnie zasilić z Centrali Sygnalizacji Pożarowej. Należy zastosować przewód wpisany w certyfikat.

Przewody i kable miedziane oraz światłowodowe wraz z ich zamocowaniami, zwane „zespołami kablowymi", stosowane w systemach zasilania i sterowania urządzeniami służącymi ochronie przeciwpożarowej, powinny zapewniać ciągłość dostawy energii elektrycznej lub przekazu sygnału przez czas wymagany do uruchomienia i działania urządzenia. Wskazane przewody i kable stosowane w obwodach urządzeń związanych z urządzeniami ppoż. powinny mieć klasę PH odpowiednią do czasu wymaganego do działania tych urządzeń, zgodnie z wymaganiami Polskiej Normy, wytycznymi CNBOP oraz obowiązującym prawem.

Wszystkie wymagane przejścia przez ściany i stropy muszą być zabezpieczone do wymaganej odporności ppoż. Na potrzeby ochrony szybów windowych projektuje się zastosowanie zasysającego systemu detekcji dymu.

Wytyczne dla inwestora i użytkownika

Użytkownik wdroży procedury na wypadek sytuacji kryzysowych umożliwiające bezpieczną ewakuację i dokończenie procedur szpitalnych z uwzględnieniem przyjętych rozwiązań technologicznych, np. procedurę bezpiecznego zakończenia operacji na wypadek alarmu pożarowego. Sugeruje się, aby drzwi przesuwne sterowane z SSP (np. na sale operacyjne, do pomieszczeń przygotowania personelu i pacjenta, itp.) nie otwierały się automatycznie, a jedynie zapewniały możliwość ręcznego ich przesunięcia – ostateczna decyzja o ewakuacji danego pomieszczenia będzie należeć do personelu.

Dodatkowo w obiekcie w pomieszczeniu z główną centralą systemu (pom. ochrony) należy zapewnić:

- Instrukcję postępowania w przypadku alarmów pożarowych oraz uszkodzeniowych;
- Plan ewakuacyjny budynku;
- Instrukcję Bezpieczeństwa Pożarowego;
- Instrukcję obsługi i konserwacji centrali;
- Skróconą instrukcję obsługi dla osoby dozorującej;
- Książkę pracy systemu;
- Wykaz niezbędnych kodów służących obsłudze centrali;
- Dokumentację systemu zawierającą opis działania, rozmieszczenie i identyfikację elementów, itp.
- Protokoły z przeglądów systemu.

Dokumentacja powinna być opisana i umieszczona w segregatorach. Dokumentacja powinna być przechowywana w szafie zamykanej drzwiami i oznakowanej jako miejsce przechowywania dokumentacji urządzeń przeciwpożarowych. W pomieszczeniu ochrony powinny znajdować się również dane kontaktowe do zarządcy budynku oraz firm wykonujących konserwacje i naprawy systemu.

W czasie odbioru Wykonawca SSP jest zobowiązany przekazać Inwestorowi następujące dokumenty:

- dokumentację powykonawczą, w której naniesiono wszelkie zmiany w stosunku do projektu wykonawczego; wszelkie zmiany powinny być uzgodnione z projektantem,
- protokoły pomiarów ciągłości instalacji, stanów izolacji oraz rezystancji linii oraz protokoły z pomiarów uziemień,
- ważne świadectwa dopuszczenia na elementy systemu.

System SSP należy regularnie poddawać przeglądom konserwacyjnym zgodnie z przepisami wytycznymi i zaleceniami producenta, a w szczególności:

sprawdzić codziennie:
- prawidłowe wskazanie dozorowania centrali,
- zapisy w książce eksploatacji dotyczące ewentualnych zmian w systemie,
- czy po ewentualnym alarmie podjęto odpowiednie działania,
- czy o ewentualnych uszkodzeniach lub odłączeniach został poinformowany konserwator, zaś centrala została przywrócona do stanu dozorowania,

sprawdzić raz w miesiącu:
- prawidłowe działanie wszystkich wskaźników (poprzez test wskaźników),
- wystarczający zapas papieru w drukarce,

zapewnić raz na kwartał aby osoby kompetentne przeprowadziły testy:
- zadziałania co najmniej jednej czujki i jednego ROPa w każdej grupie dozorowej,
- prawidłowego wyświetlania komunikatów o pobudzonych elementach oraz emitowania sygnałów optycznych i akustycznych przez centralę,
- zdatności centrali do prawidłowego sterowania i monitorowania wszystkich elementów współpracujących z systemem wykrywania pożaru,
- sprawdzić poprawność nadzorowania uszkodzeń,
- sprawdziła czy nie nastąpiły zmiany budowlane, architektoniczne, przeznaczenia pomieszczeń, bądź umeblowania mogące mieć wpływ na poprawność rozmieszczenia czujek, ROPów i sygnalizatorów.

zapewnić, aby raz w roku przeszkolony specjalista przeprowadził czynności:
- zalecane dla obsługi codziennej, miesięcznej i kwartalnej,
- sprawdzenia każdej czujki na poprawność działania przez pobudzenie (dopuszcza się raz na kwartał przetestowanie kolejnych 25% wszystkich czujek),
- sprawdzenia, czy wszystkie połączenia kablowe i aparatura są sprawne, nieuszkodzone i odpowiednio zabezpieczone,
- sprawdzenia stanu wszystkich akumulatorów.

Przeglądy okresowe (roczne, ewentualnie kwartalne) powinny być wykonywane przez wyspecjalizowany personel posiadający odpowiednie uprawnienia i wiedzę techniczną.

Właściciel, zarządca lub użytkownik obiektu lub części stanowiącej odrębną strefę pożarową, odrębnie zapewni i wdroży w myśl §6 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 roku w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. Nr 109, poz. 719), dokumentację - instrukcję bezpieczeństwa pożarowego oraz plan ewakuacji, z uwzględnieniem scenariusza rozwoju zdarzeń w czasie pożaru sporządzonym na etapie powykonawczym.

Generalny wykonawca na etapie wykonawstwa uwzględniając wytyczne projektu wykonawczego sporządzi szczegółową matrycę sterowań i scenariusz rozwoju zdarzeń w czasie pożaru. Dokument ten powinien stanowić załącznik do instrukcji bezpieczeństwa pożarowego z planem ewakuacji.

Na poszczególnych etapach powinny być sporządzone następujące rodzaje scenariuszy pożarowych:

1. scenariusze opis sekwencji możliwych zdarzeń w czasie pożaru, dla strefy pożarowej – na etapie realizacji (wykonawstwa) inwestycji - sporządza Generalny wykonawca,

2. scenariusze matryce - na etapie realizacji (wykonawstwa) inwestycji - sporządza Generalny wykonawca,
3. scenariusze powykonawcze - na zakończenie inwestycji - sporządza Generalny wykonawca; dokument ten powinien stanowić załącznik do instrukcji bezpieczeństwa pożarowego.

Odrębne dokumenty wymienione powyżej, powinny być sporządzone w określonym trybie i powinny zostać zaakceptowane przez Projektantów Projektu Budowlanego oraz uzgodnione przez rzeczoznawcę ds. zabezpieczeń przeciwpożarowych uzgadniającego Projekt Budowlany.

Minimalne parametry urządzeń

Centrala

Centrala posiada 32-bitową architekturę umożliwiającą przeniesienie znacznej części zadań sterujących do karty głównej centrali, co odciąża w dużym stopniu karty obsługującej urządzenia peryferyjne co jest stosunkowo istotne przy zaawansowanych systemach sterowania. Centrala umożliwia konfigurację do 16 podcentral połączonych z sobą w systemie kratowym z wykorzystaniem podwójnych (redundantnych) połączeń co przy pojemności jednej centrali do 14 linii dozorowych daje możliwość rozbudowy systemu do ponad 28 tyś. elementów, dzięki czemu stanowi ona idealne rozwiązanie dla rozbudowanych struktur. Do połączeń można wykorzystywać zarówno złącza z komunikacją szeregową (RS485), jak i połączenia Ethernetowe z wykorzystaniem protokołu TCP-IP. W pierwszym przypadku szybkość transmisji danych wynosi do 2,5 Mbit/s, zaś w przypadku Ethernetu do 100Mbit/s.

Gniazdo czujki

Gniazdo uniwersalne służy do podłączenia wszystkich czujek automatycznych do pętli dozorowych. Czujka jest instalowana w gnieździe za pomocą zacisku bagnetowego. Gniazdo w swojej części wewnętrznej posiada sześcio-modułowy blok zacisków, który służy do podłączenia przewodów pętli dozorowej. W przypadkach szczególnych, dodatkowe przewody można instalować do przewidzianego do tego celu modułowego bloku czterech zacisków, zamontowanego w gnieździe w uchwycie zatrzaskowym.

Blokowanie ruchomych elementów montażowych czujki następuje za pomocą zamka bagnetowego. W przypadku, gdy czujki nie są zainstalowane w gnieździe ciągłość przewodów jest zachowana (zamykana) za pomocą automatycznego mechanizmu zamykającego zintegrowanego z podstawowym blokiem zacisków. Gniazdo nie posiada automatycznego mechanizmu przełączającego dla pętli, więc obwód pętli jest zamykany tylko po zainstalowaniu czujki w gnieździe.

Interaktywna czujka multisensowa

Czujka może być stosowana jako czujka dymu, ciepła lub jako czujka dwusensorowa. Ustawienia i programowanie czujki odbywa się w zależności od obszaru zastosowania czujki. Wykrywa we wczesnym stadium tlące się ogniska pożarów, pożary otwarte, przy czym rozpoznaje i analizuje parametry dymu (wykorzystując zasadę Tyndalla) oraz temperatury (zasada sensora NTC). Do instalacji w obszarach o trudnych warunkach środowiskowych przewidziana jest wersja specjalna posiadająca podwyższoną ochronę przed wysoką wilgotnością powietrza. Posiada wbudowany izolator zwarć, dzięki któremu w przypadku przerwania przewodu lub wystąpienia zwarcia zachowane jest działanie pętli dozorowej i lokalizowane jest uszkodzenie. Jest dostarczana wraz z ochronną pokrywką przeciwpyłową.

- Alarm pożarowy po wykryciu dymu lub wzroście temperatury, lub po wykryciu dymu i wzroście temperatury
- Czujnik dymu dla automatycznej adaptacji do warunków środowiskowych bez czasochłonnego ustawiania parametrów
- Stopień czułości oraz klasa temperaturowa ustawiane zgodnie z EN54

- Analiza dymu wspierana funkcją analizy temperatury
- Analiza stanu przedalarmowego przy 30% oraz przy 75% progu alarmowym
- 2 stopniowe rozpoznania zanieczyszczenia
- Zintegrowany izolator zwarć
- Automatyczna regulacja progu zadziałania kompensująca zanieczyszczenia otoczenia
- Filtr alarmów eliminujący występowania alarmów fałszywych
- Wyjście alarmowe dla zewnętrznego wskazania alarmu
- Czas pracy i poziom zanieczyszczenia mogą być odczytywane

Moduł wejścia/wyjścia 4in 2out

Moduł ma dwa wyjście przekaźnikowe o obciążalności 2A/24VDC, 0,25A/230VAC (maks. 60W). Moduł posiada funkcję „Fail-Safe" na wypadek utraty napięcia na pętli, którą można zaprogramować dla każdego wyjścia oddzielnie. Zawiera cztery wejścia dla odczytywania stanu zestyków bezpotencjałowych. Każde wejście może być skonfigurowane z lub bez monitorowania a dodatkowo każde wejście może być zaprogramowane jako grupa dozorowa.

W celu podłączenia/zamontowania modułu na pętli dozorowej przewidziano obudowę z tworzywa sztucznego o stopniu ochrony IP 66, która posiada wiele otworów do wprowadzania przewodów. Moduł dostarczany jest razem z 8 rezystorami 180 Ω przeznaczonymi do parametryzowania wejść nadzorowanych.

Moduł wejścia/wyjścia 3in 1out

Moduł posiada wyjście przekaźnikowe z programowalnym położeniem „Fail-Safe", dwa wejścia dla odczytywania stanu zestyków bezpotencjałowych (nadzorowane lub nienadzorowane) i wejście optoizolatora, które może być zastosowane do nadzorowania napięcia zewnętrznego. Dodatkowo moduł monitoruje napięcie wewnętrzne pętli dozorowej. Adresowanie i ustawianie parametrów czujek specjalnych (np. jak zachowują się w przypadku alarmu lub awarii) jest wykonywane za pośrednictwem centrali sygnalizacji pożarowej, przy pomocy oprogramowania PC.

Moduł wyjścia 4out

Zawiera 4 przekaźniki każdy z bezpotencjałowym stykiem przełącznym o mocy 60W. Zestyki przekaźnikowe modułu mogą pracować również impulsowo. Wyjście przekaźnikowe może mieć zaprogramowane położenie „Fail-Safe", na wypadek zaniku napięcia na pętli, dodatkowo napięcie na pętli dozorowej jest monitorowane pod względem stanu podnapięcia.

Adresowanie i ustawianie parametrów poszczególnych przekaźników, jest wykonywane za pośrednictwem centrali sygnalizacji pożarowej, przy pomocy oprogramowania PC. W celu zamontowania modułu na pętli dozorowej przewidziano obudowę z tworzywa sztucznego o stopniu ochrony IP 66, która posiada wiele otworów do wprowadzenia oprzewodowania.

Czujka zasysająca

System zasysający składa się z jednej rurki ssącej, posiadającej otwory próbkujące oraz jednostki oceniającej wyposażonej w czujnik dymu. Wysokiej wydajności wentylator transportuje powietrze z nadzorowanego pomieszczenia za pomocą sieci rurek ssących do jednostki oceniającej. Stałe monitorowanie przepływu powietrza w rurce ssącej pozwala wykryć uszkodzenia rurek oraz zabrudzenia otworów próbkujących. Zasysane powietrze jest stale oceniane przez czujniki dymu zapewniając tym samym bardzo wczesne wykrycie wzrostu zawartości dymu w powietrzu. Dla każdego układu rurek zasysających można zaprogramować 3 stany prealarmu i jeden główny sygnał alarmowy, które są transmitowane do centrali za pomocą wyjść przekaźnikowych lub modułu pętlowego.

4.1.2 Dźwiękowy System Ostrzegawczy

Zakres realizacji

Na potrzeby Wielkopolskiego Centrum Zdrowia Dziecka projektuje się Dźwiękowy System Ostrzegawczy. System ten jest wymagany zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. Nr 109 poz. 719).

Zasięgiem systemu DSO objęty został cały budynek z wyłączeniem pomieszczeń gdzie system nie jest wymagany. Obszary wyłączone z instalacji systemu DSO:

- sale łóżkowe na oddziałach łóżkowych,
- sale łóżkowe na oddziałach OIOM,
- sale wybudzeniowe,
- sale operacyjne.

Projekt został opracowany zgodnie ze scenariuszem pożarowym.

Opis systemu

Podstawowe funkcje systemu DSO to automatyczne rozgłaszanie nagranych komunikatów ewakuacyjnych, ręczne rozgłaszanie komunikatów ewakuacyjnych (nagranych lub słownych) za pomocą dedykowanych mikrofonów strażaka oraz rozgłaszanie komunikatów słownych za pomocą mikrofonów informacyjnych.

Szafy sterujące systemu będą instalowane w wydzielonych pożarowo pomieszczeniach technicznych. Zastosowany system powinien posiadać możliwość rozproszonej lokalizacji urządzeń aktywnych potwierdzoną stosownymi certyfikatami. Informacja o zaistnieniu zjawiska pożarowego w poszczególnych strefach przekazywana będzie z wykorzystaniem wyjść przekaźnikowych dedykowanych modułów kontrolno-sterujących SSP.

Obiekt został podzielony na strefy nagłośnienia równoznaczne strefom pożarowym.

Alarmowe centrum pożarowe będzie zlokalizowane będzie w pomieszczeniu ochrony na parterze, w pobliżu wejścia głównego do szpitala. W tym pomieszczeniu przewidziano instalację mikrofonu strażaka do prowadzenia akcji ewakuacyjnej. Mikrofony strażaka zaprojektowano także przy szafach DSO.

Przyjęte w projekcie urządzenia oraz głośniki służące do rozgłaszania komunikatów muszą posiadać świadectwa dopuszczenia do stosowania w ochronie przeciwpożarowej na terenie Rzeczypospolitej Polskiej, wydane np. przez CNBOP w Józefowie.

Zasilanie systemu

System DSO należy zasilić kablem o cechach PH90 sprzed PWP. W szafach DSO należy przewidzieć moduły rezerwowego zasilania, które z uwagi na podłączenie systemu do awaryjnego generatora zapewnią działanie systemu przez 6 godzin w stanie bez ewakuacji i przez minimum 30 minut w stanie ewakuacji.

Automatyczne ładowanie powinno zapewnić naładowanie akumulatorów do 80% ich pojemności znamionowej w czasie nie dłuższym niż 24h od momentu ich całkowitego rozładowania.

Wykonanie systemu

Projektowany Dźwiękowy System Ostrzegania w swoich założeniach spełnia kryteria, które są zgodne z wymaganiami aktualnych norm.

Głównym zadaniem nagłośnienia jest przekazywanie komunikatów głosowych. Najistotniejszym wymaganym parametrem jest parametr zwany wyrazistością mowy. Aby uzyskać oczekiwane wartości tego parametru powyżej 0,5 STI konieczne jest m.in. zapewnienie odpowiedniego natężenia poziomu dźwięku. Projektowany system oparto na założeniach, że wymagany poziom dźwięku w danym pomieszczeniu powinien być wyższy o min. 6dB i max. 20dB od poziomu tła akustycznego.

Graniczne wartości sygnałów ostrzegawczych w całym obszarze pokrycia:

- absolutnie minimalny poziom dźwięku – 65 dBA,
- absolutnie minimalny poziom dźwięku w porze spoczynku – 75 dBA,
- słyszalność dźwięku alarmu powyżej szumu tła (stosunek odstępu sygnału od szumu) od 6dBA do 20dBA,
- maksymalny poziom dźwięku alarmu 120 dBA,
- zrozumiałość mowy w obszarze pokrycia powinna być większa albo równa 0,7 CIS (0,5 STI).

Przyjęto następujące maksymalne poziomy tła akustycznego:

- pomieszczenia techniczne głośne (maszynownie, wentylatornie itp) - 70 dB,
- pomieszczenia techniczne ciche - 65 dB,
- komunikacja - 70 dB,
- pomieszczenia administracyjne, szkolne - 60 dB,
- dyżurki pielęgniarskie, sale zabiegowe, gabinety lekarskie, toalety – 60dB.

Przyjęto następujące minimalne poziomy dźwięku dla systemu DSO:

- pomieszczenia techniczne głośne - ok. 85 dB,
- pomieszczenia techniczne ciche - ok. 75dB,
- komunikacja - ok. 85 dB,
- pomieszczenia administracyjne, szkolne - ok. 75 dB,
- dyżurki pielęgniarskie, sale zabiegowe, gabinety lekarskie, toalety - 75dBA.

Dla obiektu przyjęto podział na 35 odrębnych stref alarmowych. Strefy alarmowe zostały wydzielone zgodnie z podziałem na strefy pożarowe oraz klatki schodowe. W każdej strefie alarmowej znajduje się co najmniej jedna strefa głośnikowa. Ilość stref głośnikowych w strefie alarmowej uzależniona jest od dopuszczalnego obciążenia i długości linii. Każda strefa głośnikowa składa się z co najmniej dwóch linii głośnikowych. Z uwagi na wykorzystanie systemu DSO również do rozgłaszania komunikatów innego rodzaju niż alarmowe każda ze stref alarmowych została również podzielona na kondygnacje.

Jednostki centralne DSO znajdują się w szafach przystosowanych i certyfikowanych dla systemu DSO. Szafy wyposażone są we wszystkie niezbędne elementy takie jak: zasilacze, akumulatory, listwy, urządzenia dodatkowe. Komunikaty ewakuacyjne będą wyzwalane w sposób automatyczny po uprzednim wysterowaniu przez SSP lub przez przeszkolony personel. Z elementów kontrolno-sterujących SSP do systemu nagłośnienia podane zostaną sygnały sterujące w zależności od lokalizacji zagrożenia pożarowego. DSO w przypadku jakiegokolwiek uszkodzenia będzie przysyłał do SSP zbiorczy sygnał uszkodzenia.

W systemie zastosowano 5 mikrofonów strażaka: w pomieszczeniach central DSO oraz pomieszczeniu ochrony na parterze budynku (pom. 0.819). Dodatkowo planuje się zastosowanie mikrofonów komercyjnych do wykorzystania przez personel szpitala w celach nadawania komunikatów niezwiązanych z alarmowaniem. Mikrofony komercyjne zostają wyłączone w czasie nadawania sygnałów alarmowych.

Ze względu na specyfikę obiektu zakłada się używanie komunikatów kodowanych, skierowanych do personelu szpitala. Rozwiązanie takie podyktowane jest potrzebą zapobiegania ewentualnej panice i zdenerwowaniu pacjentów szpitala i sprawnego przygotowania ewentualnej ewakuacji.

Realizacja wszystkich funkcji wykonawczych następuje automatycznie po wykryciu przez SSP zagrożenia pożarowego lub poprzez ręczną interwencję osoby przeprowadzającej ewakuację z obiektu za pomocą mikrofonu strażaka.

Właściwości systemu

Dźwiękowy system ostrzegawczy powinien umożliwiać cyfrowe przetwarzanie sygnału audio oraz transmisję tego sygnału za pośrednictwem prostego systemu sieciowego. Transport sygnałów audio powinien odbywać się całkowicie w formie cyfrowej poza ostatnim odcinkiem linii głośnikowej 100 V. Dźwiękowy system ostrzegawczy stanowi sieciowy system zarządzania dźwiękiem. System powinien umożliwiać stworzenie 16-kanałowej sieci audio pomiędzy poszczególnymi kontrolerami systemu w oparciu o standardowe elementy sieci Ethernet. Konfiguracja sieci powinna zapewniać nadmiarowe kanały zabezpieczające, które będą zawsze przekazywać sygnały ewakuacyjne, nawet jeśli sterowniki utracą połączenie z siecią.

W każdym węźle sieci znajduje się kontroler, odpowiednia ilość routerów oraz wzmacniacze robocze i rezerwowe. Poszczególne elementy węzła łączone są w konfiguracji łańcuchowej. Węzły sieci połączone są siecią Ethernet w topologii pierścienia. Połączenia węzłów wykonuje się za pomocą niepalnych zespołów kablowych miedzianych lub kabli światłowodowych. Poszczególne moduły posiadają indywidualne adresy, które są automatycznie identyfikowane przez kontrolery. Okablowanie systemowe powinno zostać tak skonfigurowane tak, aby pojedyncza awaria w systemie nie przerywała pracy całego systemu.

Węzły sieci wyposażone są odpowiednio:

1. Szafa DSO1 - Szafa 600x600, 42U z zestawem baterii akumulatorów 2x55Ah i zasilaczem:

- 1x kontroler systemu,
- 2x router,
- 5x wzmacniacz roboczy 2x500W,
- 1x wzmacniacz rezerwowy 2x500W,
- 1x interfejs sieciowy,
- Mikrofon strażaka + klawiatury rozszerzeń.

2. Szafa DSO2 - Szafa 600x600, 42U z zestawem baterii akumulatorów 2x35Ah i zasilaczem:

- 1x Kontroler systemu,
- 2x router,
- 4x wzmacniacz roboczy 2x500W,
- 1x wzmacniacz rezerwowy 2x500W,
- 1x interfejs sieciowy,
- Mikrofon strażaka + klawiatury rozszerzeń.

3. Szafa DSO3 - Szafa 600x600, 42U z zestawem baterii akumulatorów 2x35Ah i zasilaczem:

- 1x Kontroler systemu,
- 2x router,
- 3x wzmacniacz roboczy 2x500W,
- 1x wzmacniacz rezerwowy 2x500W,
- 1x interfejs sieciowy,
- Mikrofon strażaka + klawiatury rozszerzeń.

4. Szafa DSO4 - Szafa 600x600, 42U z zestawem baterii akumulatorów 2x40Ah i zasilaczem:

- 1x Kontroler systemu,
- 2x router,
- 4x wzmacniacz roboczy 2x500W,
- 1x wzmacniacz rezerwowy 2x500W,
- 1x interfejs sieciowy,
- Mikrofon strażaka + klawiatury rozszerzeń.

Rozmieszczenie elementów systemu oraz schemat połączeń centrali DSO pokazano na rysunkach projektowych. Ostateczne lokalizacje elementów systemu, w tym szaf, w razie potrzeb należy skorygować na etapie budowy. W pomieszczeniach z centralami DSO powinno być oświetlenie awaryjne.

Opis głównych elementów systemu

Sterownik sieciowy

PODSTAWOWE FUNKCJE I PARAMETRY:

- Kontroluje i aktywuje podłączone wzmacniacze podstawowe i rezerwowe oraz zmienia przekierowania i kanały w reakcji na usterkę wzmacniacza. Łącznie kontroler informuje niezależnie o stanie 36 monitorowanych parametrów. Umożliwia określenie, które zgłaszane będą do ogólnej sumy kontrolnej błędu oraz rejestrowane w historii zdarzeń kontrolera.
- Sterownik obsługuje przełączanie na jednej linii albo w nadmiarowych grupach A/B.
- Stan połączenia sieciowego i usterki są sygnalizowane kontrolkami LED na przednim panelu.
- Urządzenie może wewnętrznie zarejestrować ponad 8000 usterek, ostrzeżeń i zdarzeń. Informacje te można oglądać na żywo oraz zapisać w pliku dziennika.
- 4 wejścia foniczne 100 V są doprowadzone do 12 wyjść linii głośnikowych. Każdy klaster 6 stref nagłośnieniowych może działać niezależnie na dwóch kanałach, umożliwiając ciągłą obecność tła muzycznego, albo na jednym kanale i w ten sposób podwajać moc nagłośnienia.
- W trybie pracy 2-kanałowej istnieje też możliwość równoległego wykonywania połączeń.
- Moc ze wzmacniacza można udostępniać wielu routerom.
- Sterownik ma wewnętrzną matrycę audio 14 x 4 z kompletną funkcjonalnością cyfrowego przetwarzania sygnału. Sterownik pracuje jako 4-kanałowa macierz wyjść.
- Pojedynczy sterownik może zarządzać 20 routerami, 16 stacjami wywoławczymi i 492 obwodami głośnikowymi.
- Można w nim skonfigurować 4 sterowane wejścia programowania.
- Wbudowany menedżer komunikatów może zapisać 100 wywołań alarmowych lub komercyjnych o łącznej długości 85 minut.
- Istnieje możliwość równoległego wysyłania dwóch różnych komunikatów do osobnych odbiorców.
- W sterowniku można zainstalować bezpłatne pliki dźwiękowe z głosowymi komunikatami ewakuacyjnymi w różnych językach. Osobne narzędzie umożliwia bieżącą zmianę komunikatów innych niż ewakuacyjne bez przerywania pracy ani restartowania systemu.
- Wyjścia stref obsługują obciążenia od 2 do 500 W.
- Maksymalna moc na 6 stref wynosi 1000 W.
- Sterownik wytrzymuje obciążenia do 2000 W.
- Możliwość podłączenia do centrali sygnalizacji pożarowej przez sieć Ethernet – dwustronnie nadzorowane połączenie z możliwością realizacji ponad 240 sterowań.
- Możliwość nagrywania w pamięci sterownika wywołań alarmowych przez 30 min - podczas stanu alarmowego.
- Możliwość programowania wyjść przekaźnikowych od zdarzeń systemowych – np. usterki wybranej linii głośnikowej celem przekazywania szczegółowych informacji nt. systemu do centrali SSP. Możliwość programowania wejść przekaźnikowych w oparciu o złożone sekwencje zdarzeń – wyzwalacz, warunek aktywacji oraz warunek zatrzymania, jako niezależnie otrzymywane sygnały. Możliwość programowania działań wyzwalanych czasowo w oparciu o wbudowany kalendarz. Możliwość programowania sekwencji zdarzeń w systemie w oparciu o funkcje logiczne.
- Otwarty interfejs do integracji z systemami automatyki budynkowej.

Router systemu

PODSTAWOWE FUNKCJE I PARAMETRY:

- Wewnętrzny układ nadzoru monitoruje działanie samego routera oraz innych urządzeń podłączonych do systemu. Przekierowuje on ruch do kanału wzmacniacza rezerwowego oraz zmienia używany kanał w reakcji na usterkę wzmacniacza.
- Przekazuje również podłączonemu sterownikowi informacje o usterkach, aby umożliwić efektywne sterowanie i rejestrowania błędów. Router obsługuje przypisanie do jednej linii albo przełączanie w nadmiarowych grupach A/B. Stan połączenia i usterki są sygnalizowane kontrolkami LED na przednim panelu, w tym kontrolką stanu strefy.
- Za pomocą routera można przekierować 4 lub więcej kanałów na 8 wejść fonicznych 100 V do 24 wyjść linii głośnikowych. Wyjścia głośnikowe routera są podzielone na klastry zawierające po 6 wyjść linii głośnikowych. Każdy klaster 6 stref może pracować na tym samym kanale lub dwóch różnych kanałach, umożliwiając odtwarzanie ciągle takiego samego lub różnego tła muzycznego w poszczególnych strefach. Każdy klaster w routerze może funkcjonować jako macierz 2-w-6 (4-kanałowa macierz wejść podłączona do 2 wejść w 6-strefowym klastrze).
- Wyjścia stref obsługują obciążenia od 2 do 500 W.
- Maksymalna moc na 6 stref wynosi 1000 W.
- Router wytrzymuje obciążenia do 4000 W.
- Wbudowana funkcja nadzoru głośników eliminuje konieczność wykorzystywania mocy wzmacniacza do nadzoru, co radykalnie obniża pobór mocy.

Wejścia foniczne (100V) Max napięcie: Max natężenie prądu: Moc maksymalna:	**AMP IN: 4x port 6-stykowy** $120V_{eff}$ 7,2 A 500W
Wyjścia foniczne (100V) Max napięcie: Max natężenie prądu: Moc maksymalna:	**SPEAKER OUT: 4x port 12-stykowy** $120V_{eff}$ 7,2 A 500W
CONTROL IN Wejścia sterujące:	**4x 10-stykowy port** - 10 wejść nadzorowanych(0–24 V, Umax= 32 V) - 10 izolowanych wejść(Niskie: U ≤ 5 V DC;Wysokie: U ≥ 10 V DC,Umaks.= 32 V)
CONTROL OUT Wyjścia sterujące: Przekaźnik sterujący:	**4x 10-stykowy port** 24 małej mocy wyjść (kolektorotwarty, Umax= 32 V, Imax=40 mA) 2 (styki przekaźnika NO/NC, Umax= 32 V, Imax= 1 A)
Interfejsy	Port CAN BUS (2x RJ-45, 10 do 500 kb/s(do sterownika, routera i wzmacniacza)
Pobór mocy	5-60W
Max prąd zasilania	<250 mA (tryb gotowości) <800 mA (Nieaktywny/Komunikat/Alarm)

Wzmacniacz

PODSTAWOWE FUNKCJE I PARAMETRY:

- wysokowydajny wzmacniacz klasy D o mocy 2x 500W. Generuje napięcia wyjść głośnikowych o wartości 70/100 V w obwodach separowanych galwanicznie.
- Wzmacniacz jest stale monitorowany przez sterownik systemowy.

- Oferuje specjalny tryb gotowości. Umożliwia on oszczędzanie energii w czasie, gdy nie jest wykorzystywana pełna funkcjonalność wzmacniacza.
- Do przesyłania sygnałów sterujących i dźwięku służą złącza RJ45.
- Dostępne cztery automatycznie wybierane wejścia foniczne realizowane przez złącze RJ45. Istnieje również możliwość wykorzystywania lokalnego wejścia bez utraty funkcjonalności nadzoru nad systemem i liniami. Wejście lokalne musi być używane w przypadku trybu autonomicznego. Wejście lokalne można skonfigurować, jako źródłowe dla zamontowanego systemu, np. zewnętrznego systemu nagłośnieniowego czy systemu wewnętrznego.
- 4 kanały wejściowe na złączu RJ45, wejście i wyjście Amp Link (dynamiczne przełączanie 4 kanałów wejściowych dla każdego wzmacniacza)
- Wbudowany ogranicznik
- Przełącznik zasilania prądem zmiennym z tyłu urządzenia

Znamionowa impedancja obciążenia (moc	
• 100 V	20 Ω (500 W)
• 70 V	10 Ω (500 W)
Znamionowa moc wyjściowa, 1 kHz, THD ≤ 1% (1)	2x 500 W
Wejściowe napięcie znamionowe	+6 dBu
Maks. wahania wartości skutecznej napięcia, 1 kHz, THD ≤ 1%, bez obciążenia	
• 100 V	110 V
• 70 V	78 V
Wzmocnienie napięcia, przy 1 kHz, stałe	
• 70 V	33,2 dB
• 100 V	36,2 dB
Maks. pojemność obciążenia	2 µF
Poziom wejścia, maks.	+18 dBu (9,75 Vrms)
Charakterystyka przenoszenia, przy 1 kHz, obciążenie znamionowe -3 dB	Od 50 do 25 kHz
Impedancja wejścia, aktywne symetryczne	20 kΩ
Stosunek sygnału do szumu (A-ważony)	> 104 dB
Poziom szumu wyjściowego (A-ważony)	< -62 dBu
Przesłuchy, przy 1 kHz	< -85 dB
Topologia stopnia wyjściowego	Klasa D, transformator,
Wymagania dotyczące mocy	
• Prąd zmienny (2)	115–240 V (-10/+10%)
• Prąd stały	21–32 V
Pobór mocy, prąd zmienny i stały	Patrz część zatytułowana „Pobór mocy” w instrukcji
Prąd rozruchowy	2 A
Prąd rozruchowy, po pięciosekundowym cyklu	1,3 A
Bezpiecznik kabla sieciowego	T6,3A (wewn.)
Bezpiecznik prądu stałego	30A (wewn.)
Awaria uziemienia	R < 50 kΩ
Port CAN BUS	2 x RJ-45, od 10 do 500 kb/s

Zabezpieczenia	Ogranicznik poziomu sygnału wejścia fonicznego, ogranicznik wyjściowej mocy skutecznej, czujnik wysokiej temperatury, zasilanie prądem stałym, zabezpieczenie przeciwzwarciowe,
Chłodzenie	Od przodu do tyłu, wentylatory sterowane termicznie
Temperatura pracy	Od -5°C do +45°C
Klasa bezpieczeństwa	Klasa I
Środowisko elektromagnetyczne	E1, E2, E3

Pobór mocy/prądu

Przy zasilaniu 230 V/50 Hz

	Izasil.	**Szasil.**	**Pzasil.**	**Pwyj.**	**BTU/h**
Tryb gotowości	0,14 A	33,0	1,9 W	0,0 W	6.5
Stan bezczynności (brak sygnału	0,20 A	47,0	19,5	0,0 W	66.5
Tryb komunikatu (–10 dB)	0,88 A	202	175 W	100 W	255.8
Alarm (–3 dB)	3,35 A	772	745 W	500 W	835.5

Przy zasilaniu 120 V/60 Hz

	Izasil.	**Szasil.**	**Pzasil.**	**Pwyj.**	**BTU/h**
Tryb gotowości	0,09 A	9,0 VA	1,3 W	0,0 W	4.4
Stan bezczynności (brak sygnału	0,27 A	29,0	17,3	0,0 W	59.0
Tryb komunikatu (–10 dB)	1,6 A	189	175 W	100 W	255.8
Alarm (–3 dB)	6,9 A	824	800 W	500 W	1023

Przy zasilaniu prądem stałym 24 V

	Izasil.	**Szasil.**	**Pzasil.**	**Pwyj.**	**BTU/h**
Tryb gotowości	0,06 A	-	1,4 W	0,0 W	4.8
Stan bezczynności (brak sygnału	0,65 A	-	15,6	0,0 W	53
Tryb komunikatu (–10 dB)	7,0 A	-	168 W	100 W	232
Alarm (–3 dB)	32,5 A	-	780 W	500 W	938

Opis kolumn w tabeli:

- Izasil. = wartość skuteczna prądu pobieranego z sieci elektrycznej (lub źródła zasilania prądem stałym),
- Szasil. = moc pozorna pobierana z sieci elektrycznej,
- Pzasil. = moc czynna pobierana z sieci elektrycznej (lub źródła zasilania prądem stałym),
- Pwyj. = moc wyjścia NF dostarczana do linii głośnikowej,
- Pstr. lub BTU/h = strata mocy przekształconej w ciepło.

Stacja wywoławcza

Do wyposażenia standardowego stacji wywoławczej należy mikrofon na wsporniku elastycznym z osłoną przeciwstukową i funkcją stałego monitorowania, podświetlany wyświetlacz ciekłokrystaliczny i zintegrowany głośnik do odtwarzania dźwięków systemu.

- Stan działania urządzenia jest stale nadzorowany przez sterownik systemu.
- Możliwość podłączenia, podłączając do niej nawet 5 zdalnych klawiatur, z których każda ma 20 dowolnie konfigurowanych przycisków funkcyjnych i wyboru.
- Stację wywoławczą można rozbudować po prawej i lewej stronie. Do stacji można również zamontować 3 dodatkowe przyciski stanu alarmowego. Opcjonalnie można także dodać przełącznik kluczykowy, który będzie blokował lub włączał funkcje stacji albo otwierał drugi poziom dostępu do urządzenia.
- Stacja ma wbudowaną klawiaturę numeryczną, którą na etapie konfigurowania można włączyć lub wyłączyć.
- Pięć przycisków menu/funkcji (zaprogramowanych fabrycznie) — na czterech przyciskach znajduje się kontrolka LED (2 są zielone, a 2 żółte).
- Zielona kontrolka LED na mikrofonie jest aktywna w trakcie połączenia.
- 15 przycisków funkcyjnych i szybkiego wybierania (konfigurowalnych) — po dwie kontrolki LED (zielona/czerwona) na każdym przycisku.
  - Na przyciskach funkcyjnych można programować m.in. następujące operacje:
  - Wybór strefy, wybór źródła, regulacja poziomu, włączanie/wyłączanie alarmów, włączanie/wyłączanie komunikatów, potwierdzanie/resetowanie po usterce.
  - Włączanie/wyłączanie wyjścia wyzwalającego lub ustawianie go w przedziale od 0 do 10 V, wybór zaplanowanych zdarzeń, włączanie/wyłączanie zaplanowanych zdarzeń.
- Pokrywa przycisków z przezroczystymi miejscami na etykiety.
- Wielojęzyczny wyświetlacz LCD informuje o stanie systemu, usterkach systemu, wybranych strefach, wyborze źródła, czasie oraz innych zdarzeniach/usterkach (za pomocą komunikatów skonfigurowanych przez użytkownika).
- Nadzorowany mikrofon elektretowy z ogranicznikiem i filtrem mowy zapewniającymi doskonałą jej zrozumiałość.
- Kabel kategorii CAT5 umożliwiający transmisję danych i dźwięku do/ze sterownika (po magistrali CAN, długość do 1000 metrów).
- Istnieje możliwość szeregowego połączenia 4 stacji wywoławczych.
- Stacja odbiera sygnały foniczne i sterujące ze sterownika, a sterownikowi wysyła informacje o swoim stanie.
- Wewnętrzny system monitorowania zdarzeń i rejestracji błędów, zgodny ze wszystkimi krajowymi i międzynarodowymi normami.
- Wejścia audio liniowe oraz mikrofonowe umożliwiające przyłączenie zewnętrznego mikrofonu lub źródła tła muzycznego.
- Głośnik stacji wywoławczej umożliwia monitorowanie aktualnie odtwarzanego sygnału audio na poszczególnych liniach głośnikowych
- Możliwość przełączania systemu w tryb stand-by i odwrotnie ze stacji wywoławczej.

Port CAN BUS	10,20 lub 62,5 kb/s, 1x RJ45, dł. Max. 1000m
Max. poziom wejściowy mikrofonu	-21 dBu
Max. poziom wejściowy linii	+4 dBu
Max. Poziom wyjściowy NF	+12 dBu
Przyciski	5 zaprogramowanych fabrycznie, 15 programowalnych przycisków stref/funkcyjnych
Kontrolki	Zasilanie (zielona), błąd (żółta), alarm (czerwona), Zielona albo żółta kontrolka

	każdego zaprogramowanego fabrycznie przycisku menu, Zielona i czerwona kontrolka każdego zaprogramowanego przycisku strefy/funkcji
Wyświetlacz ciekłokrystaliczny	Podświetlany wyświetlacz ciekłokrystaliczny (122x32 piksele)
Porty	1 port CST BUS (dane sterujące + dźwięk + zasilanie, RJ-45) 1 wejście audio (poziom liniowy, złącze jack) 1 port mikrofonu (złącze jack) 1 port EXT OUT (rozszerzenie stacji wywoławczej, RJ-12)
Zasilanie VDC	15-58V
Max prąd zasilania (bez rozszerzeń stacji wywoławczej)	Gotowość/Bezczynność/Ogłoszenie/Alert: 24V/80mA/1,92W
Max prąd zasilania (z 5 rozszerzeniami stacji wywoławczej)	Gotowość/Bezczynność/Ogłoszenie/Alert: 24V/190mA/4,56W

Klawiatura stacji wywoławczej

- Rozszerza stację o 20 konfigurowalnych przycisków funkcyjnych.
- Do jednej stacji można dołączyć maksymalnie 5 klawiatur i w ten sposób rozszerzyć stację o 100 przycisków funkcyjnych (do 115 ogółem).
- Klawiaturę można zamontować z lewej lub prawej strony stacji.
- 20 dowolnie konfigurowalnych przycisków funkcyjnych, 2 kontrolki LED (zielona/czerwona) na każdym przycisku.
- Na przyciskach funkcyjnych można zaprogramować m.in. następujące operacje:
  - Wybór strefy, wybór źródła, regulacja poziomu, włączanie/wyłączanie alarmów, włączanie/wyłączanie komunikatów, potwierdzanie/resetowanie po usterce.
  - Włączanie/wyłączanie wyjścia wyzwalającego lub ustawianie go w przedziale od 0 do 10 V, wybór zaplanowanych zdarzeń, włączanie/wyłączanie zaplanowanych zdarzeń.
- Dla kontrolek LED można zaprogramować osobną funkcjonalność sygnalizacji.
- Pokrywa przycisków z przezroczystymi miejscami na etykiety.
- Kabel RJ12 umożliwiający przesyłanie danych do stacji wywoławczej lub podłączenie innej klawiatury.
- Wysyłanie i odbieranie sygnałów sterujących do i ze stacji wywoławczej.

GŁOŚNIKI:
Głośnik sufitowy z osłoną przeciwpożarową

TABELA PARAMETRÓW ODNIESIENIA:
Czułość pasma oktawowego:

	SPL pasma oktawowego 1W/1m	Całkowite SPL pasma oktawowego 1W/1m	Całkowite SPL pasma oktawowego Pmax/1m
125 Hz	83,4	-	-
250 Hz	86,1	-	-
500 Hz	85,1	-	-
1000 Hz	87,8	-	-
2000 Hz	91,2	-	-
4000 Hz	89,7	-	-

8000 Hz	89,3	-	-
A-ważone	-	86,9	94,2
Lin-ważone	-	88,1	94,9

Kąty promieniowania pasma oktawowego:

	W poziomie	**W pionie**
125 Hz	180	180
250 Hz	180	180
500 Hz	180	180
1000 Hz	180	180
2000 Hz	120	120
4000 Hz	128	128
8000 Hz	75	75

PARAMETRY TECHNICZNE:

Moc maksymalna: 9W
Moc znamionowa: Odczepy: 6/3/1,5/0,75 W
Poziom ciśnienia akustycznego
przy mocy znamionowej/1W (1kHz,1m): 96dB/88dB (SPL)
Efektywne pasmo przenoszenia (-10dB): 85Hz – 20kHz
Kąt promieniowania przy 1kHz/4kHz (-6db): 180°/128°
Napięcie znamionowe: 100V
Impedancja znamionowa: 835/1667Ω
Temperatura pracy: -25° do 55°

Głośnik ścienny

TABELA PARAMETRÓW ODNIESIENIA:

	250Hz	**500 Hz**	**1000 Hz**	**2000 Hz**	**4000 Hz**	**8000 Hz**
SPL 1,1	84	93	94	97	97	93
SPL maks.	92	101	102	105	105	103
Dobroć Q	2,5	3,3	7,9	8,5	12,9	14,2
Skuteczność	0,32	2,2	4	7,1	5,6	2,5
Kąt zasięgu (poziom)	180	180	120	85	55	40
Kąt zasięgu (pion)	180	180	80	110	60	35

PARAMETRY TECHNICZNE:

Moc maksymalna: 9W
Moc znamionowa: Odczepy: 6/3/1,5/0,75 W
Poziom ciśnienia akustycznego
przy mocy znamionowej 6W/1W (1kHz,1m): 102dB/ 94dB (SPL)
Efektywne pasmo przenoszenia (-10dB): 150Hz – 20kHz
Kąt promieniowania przy 1kHz/4kHz (-6db): 120°/55°
Napięcie znamionowe: 70/100V
Impedancja znamionowa: 835/1667Ω
Temperatura pracy: -25° do 55°

Projektor dźwięku

TABELA PARAMETRÓW ODNIESIENIA:
Czułość pasma oktawowego:

	SPL pasma oktawowego 1W/1m	Całkowite SPL pasma oktawowego 1W/1m	Całkowite SPL pasma oktawowego Pmax/1m
125 Hz	81,1	-	-
250 Hz	88,6	-	-
500 Hz	88,3	-	-
1000 Hz	93,8	-	-
2000 Hz	96	-	-
4000 Hz	100,4	-	-
8000 Hz	94,5	-	-
A-ważone	-	93,8	105,3
Lin-ważone	-	93,8	105,7

Kąty promieniowania pasma oktawowego:

	W poziomie	W pionie
125 Hz	360	360
250 Hz	360	360
500 Hz	360	360
1000 Hz	224	224
2000 Hz	110	110
4000 Hz	56	56
8000 Hz	70	70

PARAMETRY TECHNICZNE:

Moc maksymalna: 30W
Moc znamionowa (PHC): 20W (odczepy: 20/10/5/2,5W); wyłącznie 1,25W dla 70V
Poziom ciśnienia akustycznego przy mocy znamionowej 20W/1W (1kHz,1m): 107dB/ 94dB (SPL)
Efektywne pasmo przenoszenia (-10dB): 170Hz – 20kHz
Kąt promieniowania przy 1kHz/4kHz (-6db): 224°/56°
Napięcie znamionowe: 70/100V
Impedancja znamionowa: 250/500Ω
Temperatura pracy: -25° do 55°

Liniowa matryca głośnikowa wewnętrzna

TABELA PARAMETRÓW ODNIESIENIA:

	250Hz	500 Hz	1000 Hz	2000 Hz	4000 Hz	8000 Hz
SPL 1,1	87	89	91	93	93	89
SPL maks.	102	104	106	108	108	104
Dobroć Q	1,3	202	4,5	11,6	25,7	58,9
Kąt promieniowania (poziom)	360	360	220	190	130	100
Kąt promieniowania (pion)	360	120	70	32	18	10

PARAMETRY TECHNICZNE:

Moc maksymalna: 45W
Moc znamionowa (PHC): odczepy: 30/15/7,5W); wyłącznie 1,25W dla 70V
Poziom ciśnienia akustycznego przy mocy znamionowej 30W/1W (1kHz,1m): 108dB/ 93dB (SPL)
Efektywne pasmo przenoszenia (-10dB): 190Hz – 18kHz

Kąt promieniowania przy 1kHz/4kHz (-6db): 220°/130° - poziom, 70°/18° - pion
Napięcie znamionowe: 100V
Impedancja znamionowa: 333Ω
Temperatura pracy: -25° do 55°

Liniowa matryca głośnikowa zewnętrzna

TABELA PARAMETRÓW ODNIESIENIA:

	250Hz	500 Hz	1000 Hz	2000 Hz	4000 Hz	8000 Hz
SPL 1,1	94	97	97	95	96	93
SPL maks.	112	115	115	113	114	111
Dobroć Q	2,2	2,7	6,3	10,8	22,6	32,3
Kąt promieniowania (poziom)	360	180	170	160	90	60
Kąt promieniowania (pion)	100	60	55	34	18	10

PARAMETRY TECHNICZNE:

Moc maksymalna: 90W
Moc znamionowa (PHC): odczepy: 60/30/15W)
Poziom ciśnienia akustycznego przy mocy znamionowej 60W/1W (1kHz,1m): 115dB/ 97dB (SPL)
Efektywne pasmo przenoszenia (-10dB): 190Hz – 20kHz
Kąt promieniowania przy 1kHz/4kHz (-6db): 170°/90° - poziom, 55°/18° - pion
Napięcie znamionowe: 100V
Impedancja znamionowa: 167Ω
Temperatura pracy: -25° do 55°

Wytyczne dla inwestora i użytkownika

Użytkownik wdroży procedury na wypadek sytuacji kryzysowych umożliwiające bezpieczną ewakuację i dokończenie procedur szpitalnych z uwzględnieniem przyjętych rozwiązań technologicznych, np. procedurę bezpiecznego zakończenia operacji.

Dodatkowo w obiekcie należy zapewnić:

- instrukcję obsługi systemu,
- książkę eksploatacji systemu, do której należy wpisywać: okresowe kontrole instalacji i urządzeń, dokonane naprawy, zmiany i uzupełnienia instalacji, wszystkie alarmy z podaniem daty i godziny ich wystąpienia, wyłączenia głośników, stref i linii,
- instrukcję organizacji alarmowania na budynku,
- rozpisany podział głośników z przypisaniem ich do odpowiednich pomieszczeń, czyli tzw. legenda systemu,
- dokumentację techniczną (powykonawczą) systemu zawierającą opis jego działania, sposób zasilania, umożliwiającą łatwą identyfikację linii głośnikowych, stref, objętych pomieszczeń oraz innych elementów systemu,
- opis producenta (w języku polskim) DTR użytkownika.

W czasie odbioru Wykonawca DSO jest zobowiązany przekazać Inwestorowi następujące dokumenty:

- dokumentację powykonawczą, w której naniesiono wszelkie zmiany w stosunku do projektu wykonawczego; wszelkie zmiany powinny być uzgodnione z projektantem i rzeczoznawcą,

- protokoły pomiarów ciągłości instalacji, stanów izolacji oraz rezystancji linii oraz protokoły z pomiarów uziemień,
- ważne świadectwa dopuszczenia na elementy systemu.

System DSO należy regularnie poddawać przeglądom konserwacyjnym zgodnie z przepisami wytycznymi i zaleceniami producenta. Przeglądy okresowe powinny być wykonywane przez wyspecjalizowany personel posiadający odpowiednie uprawnienia i wiedzę techniczną. Niedopuszczalne jest wykonywanie przez użytkownika (bez zgody producenta systemu) jakichkolwiek modyfikacji w poszczególnych urządzeniach i okablowaniu systemu.

4.1.3 Instalacja sieci strukturalnej

Przyłącze

Na potrzeby uzyskania dostępu do sieci telekomunikacyjnej przewiduje się wykorzystanie przyłącza telekomunikacyjnego. Okablowanie operatora/operatorów należy doprowadzić do budynku do pomieszczenia przyłącza, następnie do projektowanego Głównego Punktu Dystrybucyjnego zlokalizowanego w pom. serwerowni (IT room). W pomieszczeniu przyłącza zaprojektowano szafkę dedykowaną dla operatorów wraz z wyposażeniem pasywnym.

Ogólne założenia systemu

Zakłada się topologię systemu w oparciu o pomieszczenie serwerowni na najniższej kondygnacji oraz Pośrednie Punkty Dystrybucyjne (PPD) rozmieszczone w pozostałej części budynku na poszczególnych piętrach. Przewiduje się po trzy PPD na każdej kondygnacji nadziemnej oraz jeden PPD na kondygnacji podziemnej.

W celu wykorzystania najwyższych możliwości projektowanego systemu, standard i technologię dobrano na podstawie wytycznych normy określającej okablowanie strukturalne w ośrodkach medycznych ANSI/TIA-1179. Norma rekomenduje m.in. wydajności 10Gb/s, minimalną klasę okablowania EA S/FTP. Ponadto należy, stosować redundancję i nadmiarowość połączeń dwoma różnymi trasami z pomieszczeniem teletechnicznym.

4.1.3.1 Opis części aktywnej

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:

- automatyki budynkowej,
- kontroli dostępu,
- systemu CCTV, pracujących z wykorzystaniem protokołów IP, jak i innych elementów systemów bezpieczeństwa obiektu,
- systemów i aplikacji wykorzystywanych, bądź przewidywanych do wykorzystania w przyszłości w budynku Szpitala, w tym wideokonferencji,
- 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 rekonfiguracje i modyfikacje, na potrzeby realizacji potrzeb systemów i aplikacji Szpitala.

Architektura zaprojektowanej sieci opiera się na strukturze wielowarstwowej, zarówno dotyczy to skalowalności sieci (wielkości przepustowości, mocy przetwarzania wykorzystywanych urządzeń), jak i protokołów (wykorzystywanie technologii L2/L3/L4 – Layer 2/3/4 Switching). Należy zwrócić uwagę, że realizowane warstwy sieci, są warstwami logicznymi, przez co projektowane urządzenia sieciowe mogą być współdzielone przez dwie, a nawet więcej warstw. Stworzenie architektury warstwowej sieci lokalnej ułatwia jej skalowanie, podłączanie nowych węzłów sieci, jak i migrację sieci komputerowych w kierunku nowych technologii i rozwiązań sieciowych, zgodnie z przyszłymi wymaganiami technologii wykorzystywanych w Szpitalu. Tak stworzona struktura sieci pozwala na wykorzystanie zaawansowanych technik zabezpieczających sieć przed przerwą pracy w przypadku awarii. Ponadto ułatwia na skalowanie przepustowości 10/100/1000/10/25 i 40Gb/s, a w przyszłości również 100Gb/s, w zależności od lokalizacji, jak i umiejscowienia urządzenia w sieci.

W realizowanej topologii sieci lokalnej w Szpitalu, sieć lokalna oparta jest na standardach Ethernet: 10/100/1000/10G/40G, wraz z agregacją kanałów Gigabit Ethernet, zgodnie ze standardem IEEE 802.3ad. Zaletą wykorzystania tej technologii w szkielecie sieci jest jej wydajność i grupowanie łączy w logiczne grupy, umożliwiając tym samym skalowanie pasma przepustowości pomiędzy węzłami sieci, w zależności od potrzeb w przyszłości, z zachowaniem redundancji połączeń i automatyzacji przełączenia w przypadku awarii. Ponadto dodatkowe standardy QoS, pozwalają na strojenie sieci komputerowej do wymagań usług sieciowych (w tym do wymagań telefonii IP, systemu CCTV), jak i polityki bezpieczeństwa. W ramach projektowanej sieci, zakłada się możliwość uzupełnienia poszczególnych kanałów agregujących połączenia, w przyszłości, zgodnie z wymaganiami i rozwojem systemów w Szpitalu, bez konieczności dołożenia dodatkowych przełączników (poza warstwą agregującą/szkieletem sieci LAN), a wyłącznie w oparciu o dołożenie odpowiednich modułów SFP/SFP+/QSFP.

Model warstwowy, szczególnie przy wykorzystaniu możliwości warstwy sieciowej, pozwala na elastyczne, jak również dość efektywne zaprojektowanie łączy zapasowych, czy też komunikacji w przypadku pojedynczej awarii. Redundancja łączy jak i urządzeń sieciowych, realizowana jest począwszy od warstwy szkieletowo – dystrybucyjnej, skończywszy na warstwie dostępowej, w poszczególnych punktach dystrybucyjnych w budynku. Niewątpliwą zaletą jest możliwość wykorzystywania łączy zapasowych nie tylko w czasie awarii łączy podstawowych, ale również w czasie normalnej ich pracy, tworząc grypy łączy pomiędzy poszczególnymi węzłami sieci, zwiększając przepustowość połączenia do infrastruktury serwerowej, wykorzystywanej w Szpitalu.

Jednym z istotniejszych założeń 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 pracujących w Szpitalu.

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 i systemów pracujących w Szpitalu.

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:

1. Struktura fizyczna zintegrowanej sieci LAN, na potrzeby podłączania poszczególnych systemów teletechnicznych, jak również użytkowników i systemów innych systemów wykorzystywanych w Szpitalu, biorąc pod uwagę między innymi różną rolę do spełnienia, jak również różne delegacje uprawnień w ramach infrastruktury sieciowej, zakłada się, że składa się z:

- warstwy dystrybucyjno-szkieletowej, zgodnie z wymaganiami przedstawionymi w dalszej części projektu,
- warstwy dostępowej, z uwzględnieniem podziału na części bezpieczeństwa - Security i pozostałe systemy,
- warstwy na potrzeby wydajnego podłączenia serwerów i systemów zarządzania infrastrukturą sieciową,
- warstwy na potrzeby realizacji styku z siecią Internet i inne sieci zewnętrzne, z uwzględnieniem możliwości komunikacji w oparciu o dynamiczne protokoły routingu.

2. Warstwa dostępowa, na potrzeby przyłączenia poszczególnych urządzeń sieciowych, rozlokowanych w punktach dystrybucyjnych na poszczególnych piętrach, zarówno dla systemów bezpieczeństwa, jak i dla użytkowników końcowych, czy innych systemów (za wyjątkiem warstwy dostępu dla serwerów) zbudowana jest w oparciu o jednolitą platformę sprzętową i programową, przy czym połączenia szkieletowe, zróżnicowane są per system:

- dla systemu bezpieczeństwa, zakłada się agregację połączeń 1Gb/s, opartą na połączeniach SMF (ang. Single Mode Fiber),
- dla pozostałych systemów, oparte o agregację połączeń 10Gb/s, opartych na połączeniach SMF,
- w zależności od potrzeb, zagregowanych w oparciu o odpowiednie ilości połączeń fizycznych, zgodnie z wymaganiami przedstawionymi dla poszczególnych punktów dystrybucyjnych sieci.

3. W ramach budowy warstwy dostępowej, dla poszczególnych punktów dystrybucyjnych, zakłada się budowę logicznych stosów urządzeń (szczegółowe wymagania przedstawione są w dalszej części projektu), w celu ujednolicenia zarządzania i konfiguracji urządzeń (usprawni to późniejszą administrację i utrzymanie spójności konfiguracji węzłów sieci LAN, w tym polityk bezpieczeństwa i zapewnienia jakości komunikacji w sieci lokalnej dla poszczególnych systemów).

4. Warstwa dostępowa dla poszczególnych systemów, zakłada dostarczenie odpowiedniego poziomu zasilania, zgodnego ze standardem Power over Ethernet Plus (PoE+), dla wymagających tego systemów. W tym zakłada się, uzupełnienie warstwy dostępowej o odpowiednie rozwiązania w celu realizacji połączeń światłowodowych na zewnątrz i wewnątrz budynku – podłączenia urządzeń końcowych w oparciu o połączenia światłowodowe.

5. W ramach budowy warstwy szkieletowej, zakłada się stworzenie warstwy agregacyjnej dla części sieci Security, jak również warstwy szkieletowej, spinającej wszystkie systemy i aplikacje wykorzystywane w ramach Szpitala, przy zachowaniu odpowiedniego poziomu kontroli, separacji jak i bezpieczeństwa poszczególnych systemów. W poszczególnych warstwach agregacyjnej/szkieletowej zakłada się odpowiednią liczbę połączeń SMF 1Gb/s i 10Gb/s, zgodnie ze szczegółową specyfikacją przedstawioną w dalszej części projektu.

6. W ramach warstwy sieciowej, na potrzeby podłączenia serwerów, systemów zarządzania i utrzymania sieci, zakłada się strukturę realizowaną w topologii ToR (ang. Top of Rack), z portami 1/10Gb/s, realizowanymi w standardzie UTP. Jednocześnie podłączenie do szkieletu sieci, oparte jest na standardzie 40Gb/s, w celu zapewnienia odpowiedniego poziomu wydajności połączeń z poszczególnych punktów dystrybucyjnych do systemów i aplikacji, podłączanych w serwerowni głównej – GPD.
7. Systemy zarządzania/utrzymania/monitorowania aplikacji jak i kontroli dostępu do sieci, dla poszczególnych systemów, podłączane są w centralnym punkcie dostępu do sieci – GPD, z uwzględnieniem wstępnie zakładanych wydajności i ilości jednocześnie zarządzanych urządzeń końcowych sieci LAN i WLAN. Wstępne założenia przedstawione są szczegółowo w dalszej części projektu.
8. 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 w Szpital. Minimalne wymagania na integrację poszczególnych systemów, zostały przedstawione w dalszej części projektu.
9. W poszczególnych punktach dystrybucyjnych zakłada, się na potrzeby monitorowania/bezpieczeństwa systemów i węzłów sieci LAN, jak również dostępu do sieci komputerowej, dedykowane dla administratorów sieci, systemy monitorowania wizyjnego, jak również systemu dostępu bezprzewodowego do sieci LAN. Zakłada się, że systemy te będą zintegrowane ze sobą (mogą być urządzenia realizujące obie funkcjonalności jednocześnie), przy założeniu potencjalnej możliwości integracji z ogólnych systemem Security, wykorzystywanym w Szpitalu.
10. Zaprojektowana sieć bezprzewodowa realizuje funkcje lokalizacji, na wyznaczonych piętrach, z zachowaniem standardów 802.11 b/g/n/ac/ac-wave2. Zarządzanie poszczególnymi punktami dostępu do sieci bezprzewodowej odbywa się z poziomu redundantnego kontrolera, realizowanego w postaci zwirtualizowanej.
11. Warstwa kontroli poszczególnych punktów dostępu do sieci bezprzewodowej, oparta jest na redundantnym systemem kontrolera, w postaci zrytualizowanej, pracującym w trybie active/active.
12. Zasilanie dla poszczególnych punktów dostępu do sieci bezprzewodowej odbywa się poprzez standard Power over Ethernet, z poziomem mocy wymaganym 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.
13. Styk z sieciami zewnętrznymi, w tym z siecią Internet, odbywa się z wykorzystaniem urządzeń typu NGFW (ang. New Generation Firewall), pracujące w klastrze niezawodnościowym HA (ang. High Availability), mającymi na celu zwiększenie niezawodności i sterowalności podłączenia i wyboru trasy (routingu). Szczegółowa specyfikacja wymagań przedstawiona zostały w dalszej części projektu. Przy czym należy uwzględnić nie tylko realizacje poszczególnych funkcjonalności w ramach tzw. NGFW, ale również możliwość separacji poszczególnych środowisk, w oparciu o wirtualne instancje firewalla, w celu odpowiedniego poziomu separacji środowisk, w tym między innymi, w razie potrzeby:

- środowiska użytkowników końcowych, pracowników Szpitala itp.,
- środowiska systemów CCTV,
- środowiska systemów teletechnicznych,

- styku z sieciami zewnętrznymi,
- styku z siecią Internet, z uwzględnieniem w razie potrzeby stref DMZ.

Wymagania szczegółowe dla poszczególnych punktów dystrybucyjnych

Poniżej zostały przestawione wymagania na ilości i rodzaje poszczególnych systemów, z podziałem na odpowiednie punkty dystrybucyjne. Przy czym szczegółowe wymagania dotyczące poszczególnych urządzeń, wykorzystywanych dla systemów przedstawione są w dalszej części projektu, w tym wymagania związane między innymi z integracją pomiędzy poszczególnymi systemami.

Poszczególne przełączniki sieciowe zarówno na potrzeby dostępu Security, jak i na potrzeby pozostałych systemów, powinny pochodzić z jednej rodziny przełączników, zapewniając tym samym spójność i jednolitość konfiguracji sieciowej. Jednocześnie spójność zastosowanych rozwiązań, zapewnia elastyczność w czasie utrzymania i rozbudowy poszczególnych węzłów sieci LAN, jak i odpowiednich komponentów do zarządzania infrastrukturą sieciową, jak i bezpiecznym dostępem do niej.

W zakresie poszczególnych punktów dystrybucyjnych zakłada się, dostarczenie następujących urządzeń i systemów, przedstawionych w tabeli poniżej. Szczegółowe wymagania dla poszczególnych urządzeń zostały przedstawione w kolejnych podpunktach, z rozbiciem rodzajów i typów urządzeń, per wymagana warstwa w ramach topologii/architektury sieci.

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
GPD - Serwerownia	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 3 x 10GBASE SFP+ (kabel passive copper: 2x 1m, 1 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik Security: 48x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	4 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security 9 x 1GBsae-LX – połączenia światłowodowe na potrzeby podłączenia systemów zewnętrznych security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 3 x 10GBASE SFP+ (kabel passive copper: 2x 1m, 1 x3m).
	Przełącznik Security: 48x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Przełacznik Security: 24 porty 1000Base-X, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	29	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
	Przełącznik szkieletowy LAN: 48x10GBASE-X SFP+, 4x40GBASE-X QSFP+	2	84 x 10GBase-LR SFP+ 2 x 40GBASE passive cable 5m	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 40GBASE QSFP+ (kabel passive copper: 2x 5m). Zasilacze redundante per przełącznik sieciowy. Redundante wentylatory.
	Przełącznik agregujący Security: 48x1000BASE-X, 4 x10GBASE-X SFP+	2	48x1000Base-LX SFP, 4x10GBase-LR SFP+ 2x10GBase-X passive cable 1m	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+. Zasilacze redundante per przełącznik sieciowy. Redundante wentylatory.
	Przełącznik ToR na potrzeby podłączenia serwerów: 48 x 1G/10G BASE-T, 2 x 10G/40GBASE-X QSFP+, 4 x 10G/25G/40G/50G/100GBASE QSFP28	2	2 x 40GBASE-X QSFP+ passive cable – 3 m, 2 x 10G SFP+, passive Cable 5 m	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 40GBase QSFP+ (2 x kabel passive 5m). Zasilacze redundante per przełącznik sieciowy.

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
				Redundante wentylatory.
	System do zarządzania infrastrukturą LAN/WLAN	1	100 urządzeń węzłów sieci LAN do 1000 AP sieci WiFi	Pracujące na serwerze przedstawionym poniżej, **w postaci maszyny wirtualnej**, na maszynie wirtualnej.
	System NAC – wersja zaawansowana	1	Do 3k urządzen końcowych jednocześnie zarządzanych	System uruchomiony na serwerze, **w postaci maszyny wirtualnej** na maszynie wirtualnej
	System NAC – posture	1	Do 3k urządzen końcowych jednocześnie zarządzanych	System uruchomiony na serwerze, w postaci maszyny wirtualnej **na systemie wirtualizacyjny**
	System/aplikacja do zarządzania AP sieci WLAN	2	Zapewniający zarządzanie całościowej liczby AP. Zakłada się wstępnie nieprzekroczenie 500 AP w pojedynczym systemie	System uruchomiony na serwerach, w postaci maszyny wirtualnej **na systemie wirtualizacyjnym**, pracujący w trybie HA
	Serwer do zamontowania w szafie rack, z licencją na system wirtualizacyjny – silnik do wirtualizacji zasobów sprzętowych	2	2 (dwa serwery) x 2 porty w standardzie 10GBase-T, w celu podłączenia do infrastruktury sieciowej – do przełączników serwerowych ToR	System do wirtualizacji zasobów pozwalający na uruchomienie maszyn wirtualnych z poszczególnymi aplikacjami i systemami, jak powyżej
	Media konwerter pracujący w standardzie 1x10/100/1000Base-T/1GBase-X pracujących w warunkach przemysłowych, dla 1 urządzenia wymagane zasilanie PoE na poziomie 60W – dla urządzeń końcowych	6 – media konwerter 1 – media konwerter z PoE na poziomie 60W	7 x 1GBase-LX	Urządzenia montowane na szynie DIN, pracujące w warunkach przemysłowych (zakres temperatur) z zapewnieniem zasilania dla urządzeń na poziomie 60W – możliwe jest zastosowanie urządzeń zapewniających obie funkcjonalności w dwóch modułach
	Firewall typu NGFW, z zapewnieniem wirtualnych kontekstów, w celu separacji elementów bezpieczeństwa, zgodnie z wymaganiami	2	4 x 10GBASE-X SFP+	Klaster urządzeń, z zapewnieniem funkcjonalności opisanych w dalszej części projektu
	Serwer do zarządzania infrastrukturą telefoniczną – centrala IP, pracująca na systemie wirtualizacyjnym	2	8 x 1GBASE-T	Klaster urządzeń, z funkcjonalnościami do realizacji funkcjonalności centrali telefonicznej i systemu faksowego
	Brama głosowa – realizująca styk z sieciami zewnętrznymi – połączenia cyfrowe ISDN E1	2	2 x 1GBASE-T	System do realizacji funkcjonalności komunikacji pomiędzy szpitalem i systemami zewnętrznymi telefonicznymi, w oparciu o połączenia cyfrowe ISDN
PPD.-1.3	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper: 4x 1m, 1 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	3		
	Przełącznik Security: 12x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	4 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security 13 x 1GBsae-LX – połączenia światłowodowe na	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 3 x 10GBASE SFP+ (kabel passive copper: 2x 1m, 1 x3m).
	Przełącznik Security: 48x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
	Przełacznik Security: 24 porty 1000Base-X, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	potrzeby podłączenia systemów zewnętrznych security	
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	26	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
	Media konwerter pracujący w standardzie 1x10/100/1000Base-T/1GBase-X pracujących w warunkach przemysłowych, dla 3 urządzenia wymagane zasilanie PoE na poziomie 60W – dla urządzeń końcowych	10 – media konwerter 3 – media konwerter z PoE na poziomie 60W	7 x 1GBase-LX	Urządzenia montowane na szynie DIN, pracujące w warunkach przemysłowych (zakres temperatur) z zapewnieniem zasilania dla urządzeń na poziomie 60W – możliwe jest zastosowanie urządzeń zapewniających obie funkcjonalności w dwóch modułach
PPD.0.1	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	8 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 7 x 10GBASE SFP+ (kabel passive copper: 5x 1m, 2 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	6		
	Przełącznik Security: 48x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	2	4 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security 8 x 1GBsae-LX – połączenia światłowodowe na potrzeby podłączenia systemów zewnętrznych security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	18	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
	Media konwerter pracujący w standardzie 1x10/100/1000Base-T/1GBase-X pracujących w warunkach przemysłowych (zakres temperatur)	6	6 x 1GBase-LX	Montowany na szynie DIM, pracujący w warunkach środowiskowych przemysłowych (zakres temperatury). Dla 4 urządzeń zapewnione dodatkowo zasilanie PoE na poziomie 60W.
PPD.0.2	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 4 x 10GBASE SFP+ (kabel passive copper: 3x 1m, 1 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	2		
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	15	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.0.3	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 6 x 10GBASE SFP+ (kabel passive copper: 5x 1m, 1 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	4		
	Przełącznik Security: 48x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1	warstwy dystrybucyjnej Security	10GBASE SFP+ (kabel passive copper: 2x 1m).
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	15	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.1.1	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 6 x 10GBASE SFP+ (kabel passive copper: 5x 1m, 1 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	5		
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	19	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.1.2	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 4 x 10GBASE SFP+ (kabel passive copper: 3x 1m, 1 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	2		
	Przełącznik Security: 48x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	15	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.1.3	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 6 x 10GBASE SFP+ (kabel passive copper: 5x 1m, 1 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	4		
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	15	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.2.1	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	8 x 10GBase-LR – połączenie do warstwy szkieletowej LAN 44x1GBase-LX – połączenia do sal	Stworzenie 2 stosów przełączników sieciowych, w oparciu o dedykowane połączenia 11 x 10GBASE SFP+ (kabel passive copper: 9x1m, 2 x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x1000BASE-X, 4x10GBASE-X SFP+	1		

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	9	operacyjnych w oparciu o dedykowane światłowody	
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	15	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.2.2	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 4 x 10GBASE SFP+ (kabel passive copper: 3x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	3		
	Przełącznik Security: 12x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	12	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.2.3	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper: 4x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	4		
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	9	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.3.1	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 6 x 10GBASE SFP+ (kabel passive copper: 5x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	5		
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	17	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.3.2	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 3 x 10GBASE SFP+ (kabel passive copper: 2x1m,

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	2	LAN	1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik Security: 48x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	15	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.3.3	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper: 4x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	4		
	Przełącznik Security: 48x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	14	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.4.1	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper: 4x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	3		
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	19	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.4.2	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 4 x 10GBASE SFP+ (kabel passive copper: 3x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	2		
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	14	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
PPD.4.3	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper: 4x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	4		
	Przełącznik Security: 12x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	14	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.5.1	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 8 x 10GBASE SFP+ (kabel passive copper: 7x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	7		
	Przełącznik Security: 24x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 48x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	18	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.5.2	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 3 x 10GBASE SFP+ (kabel passive copper: 3x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	2		
	Przełącznik Security: 12x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 10GBASE SFP+ (kabel passive copper: 2x 1m).
	Przełącznik Security: 24x10/100/1000BASE-T, 4 x1GBASE-X SFP	1		
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	14	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
PPD.5.3	Przełącznik LAN: 24x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	1	4 x 10GBase-LR – połączenie do warstwy szkieletowej LAN	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 6 x 10GBASE SFP+ (kabel passive copper: 5x1m, 1x3m). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T, 4x10GBASE-X SFP+	5		
	Przełącznik Security: 48x10/100/1000BASE-T POE+, 4 x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy dystrybucyjnej Security	-
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	14	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.

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 oraz uruchomionymi w sieci usługami. Zasadniczymi zadaniami systemu będą monitorowanie stanu infrastruktury, centralizacja procesów zarządzania i konfiguracji urządzeń sieciowych, kontrolowanie i uwierzytelniania podłączających się do infrastruktury urządzeń końcowych oraz monitorowanie usług i aplikacji działających w sieci.

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, urządzenia sieci szkieletowej, urządzenia bezprzewodowej sieci WLAN oraz systemy zabezpieczeń sieciowych (takie jak zapora sieciowa firewall - NGFW).

System stanowić będzie centralny punkt zarządzania infrastrukturą sieciową poprzez graficzny interfejs www. System zarządzania wykorzystywany będzie do konfiguracji urządzeń infrastruktury dostępowej i szkieletowej, 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 służył 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.

System musi umożliwiać również monitorowanie stanu urządzeń końcowych po uzyskaniu połączenia z siecią pod kątem:

- weryfikacji zainstalowanego oprogramowania antywirusowego,
- weryfikacji aktualności sygnatur antywirusowych,
- weryfikacji aktualności poprawek systemu MS Windows,
- weryfikacji wpisów w rejestrze systemu,
- weryfikacji uruchomionych serwisów,
- weryfikacji uruchomionych aplikacji,
- weryfikacji otwartych portów.

W przypadku niezgodności systemu końcowego z założoną polityką bezpieczeństwa powinno nastąpić przypisanie użytkownikowi polityki kwarantanny, a następnie proces naprawy. Proces naprawy (aktualizacji stacji) realizowany musi być automatycznie z odpowiednim powiadomieniem użytkownika o kwarantannie, przyczynie i statusie naprawy.

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, objętą niniejszym postępowaniem. W zamyśle projektuje się, by była automatyzacja działań prewencyjnych oraz wymiana informacji pomiędzy różnymi systemami bezpieczeństwa sieciowego. System musi automatycznie podejmować działania prewencyjne i izolacyjne (poprzez przeniesienie do kwarantanny) urządzenia lub użytkownika, który złamie regułę systemu firewall (m.in. pobierze z sieci podejrzane oprogramowanie lub plik, połączy się z zabronioną stroną sieci web itp.).

System musi umożliwiać analizę 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.

Rozwiązanie powinno umożliwiać uzupełnienie, poza niniejszym postępowaniem, infrastruktury o dodatkowe rozwiązanie, dedykowane do zbierania dużej ilości danych typu Netflow, w pełni zintegrowane z niniejszym rozwiązaniem zarządzania.

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.

Poniżej znajdują się szczegółowe wymagania per system zarządzania/monitorowania uwzględniony w ramach niniejszego projektu.

Wymagania szczegółowe dla systemu zarządzania siecią LAN i WLAN

Poniżej zostały zawarte szczegółowe wymagania, realizowane w ramach projektowane systemu zarządzania infrastruktura sieciową, jej poszczególnymi komponentami sieci LAN i WLAN.

Funkcjonalność systemu zarządzania siecią i poszczególnymi urządzeniami

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

Architektura

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

Raportowanie

1. Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci.
2. Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (OID).
3. Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).
4. Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia.
5. Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu.

6. Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu firmware urządzenia.
7. Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń.
8. Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych.
9. Musi zapewniać możliwości analiz na poziomie portu.
10. Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów.

Narzędzia administracyjne

1. Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania.
2. 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.
3. Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby.
4. Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania firmware i wielkość pliku konfiguracyjnego.
5. Musi posiadać możliwość pobierania oprogramowania firmware do jednego urządzenia lub do wielu urządzeń jednocześnie.
6. Musi mieć możliwość pobierania obrazów boot PROM do jednego urządzenia lub do wielu urządzeń jednocześnie.
7. Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń.
8. Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń.
9. Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania.
10. Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury.
11. Musi umożliwiać automatyczną reakcję w czasie rzeczywistym poprzez integrację z rozwiązaniami klasy SIEM oraz IPS.
12. Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym.

Bezpieczeństwo

1. Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji.
2. Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https.
3. 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

4. Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą aplikacji, dzięki której polityki zostaną rozesłane do wszystkich urządzeń.
5. Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci.
6. Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC.
7. Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p.
8. Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania.
9. Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku.
10. Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 Trap (Inform).
11. Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS.

Kontrola

1. Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia.
2. Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci.
3. Musi mieć możliwość przypisania „roli kwarantanny" użytkownikowi podłączonemu do portu.
4. Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji.
5. 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 minimum 100 urządzeń sieciowych i do 1000 urządzeń dostępu do sieci bezprzewodowej oraz umożliwiać w przyszłości rozbudowę do min. 250 urządzeń sieciowych – węzłów sieci LAN.

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 otwartych strukturach sieci, do których należy projektowana w Szpitalu, jest to bardzo istotny

komponent sieciowy, zwiększający poziom bezpieczeństwa wykorzystywanych systemów, jak i zwiększający kontrolę aplikacji i komunikacji dla poszczególnych użytkowników sieci.

Funkcjonalność

1. System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem:

- standardu 802.1X
- adresu MAC urządzenia
- formularza webowego

2. System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) 802.1X opartych o złożone i wielowarunkowe reguły profili bezpieczeństwa.
3. System powinien aktywne zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów.
4. System powinien współpracować z rozwiązaniem Microsoft NAP (Network Access Protection).
5. 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.
6. Musi zapewniać możliwość powiadamiania poprzez Syslog oraz pocztę elektroniczną o sytuacjach krytycznych.
7. System musi umożliwiać wysyłanie powiadomień mailowych z wykorzystaniem protokołu SMTP.
8. System musi posiadać wewnętrzną bazę użytkowników. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych przy pomocy interfejsu programistycznego.
9. Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania i autoryzacji podłączanych systemów końcowych.
10. Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i/lub LDAP.
11. Rozwiązanie musi obsługiwać lokalną autoryzację MAC.

Profilowanie urządzeń

1. 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.
2. System musi umożliwiać dodawanie rozpoznanych urządzeń do grupy.
3. 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 500 urządzeń.
4. 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

1. System musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych i/lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości stopniowego zwiększania wydajności systemu.
2. 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.
3. 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.
4. 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.
5. Musi być dostarczone jako maszyna wirtualna lub jako dedykowane rozwiązanie sprzętowe.
6. System musi umożliwiać obsługę co najmniej 3000 urządzeń równocześnie podłączonych do sieci lokalnej LAN oraz sieci bezprzewodowej WLAN.
7. Rozwiązanie powinno wspierać możliwość rozbudowy do min. 6000 sesji autoryzacyjnych bez potrzeby rozbudowy systemu o dodatkowe serwery fizyczne lub wirtualne - poprzez dodanie do systemu odpowiednich licencji.
8. System musi umożliwiać ocenę stanu zabezpieczeń systemu końcowego (dla min. 3000 systemów końcowych). Ocenianie musi być możliwe zarówno bez dedykowanego agenta instalowanego na stacji końcowej jak i z użyciem agenta.
9. Ocenianie w oparciu o agenta dostępnego 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).

10. Musi być 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.
11. Podczas oceniania systemu końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów.
12. 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
13. Musi być możliwość przeniesienia systemu końcowego do kwarantanny w razie braku połączenia agenta z serwerem systemu kontroli dostępu do sieci
14. System końcowy podlegający kwarantannie musi otrzymać informację o testach zakończonych niepowodzeniem wraz ze wskazówkami ich poprawienia
15. Administrator musi mieć możliwość określenia punktacji oraz progu kwarantanny każdego testu wraz z jego charakterem (informacyjny, ostrzeżenie, wymagany do spełnienia).

Zarządzanie systemem

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

Zarządzenie dostępem gościnnym

1. 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.
2. Rozwiązanie musi posiadać funkcję portalu rejestracyjnego, aby zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT.
3. Możliwość sponsorowania dostępu takie jak sponsorowanie email wraz z portalem dla sponsorów służący do zatwierdzania rejestracji gości.
4. Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych o wybranej długości, mogących składać się z różnego rodzaju znaków.
5. 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.

6. System musi umożliwiać dopasowanie wyglądu portalu wybranym użytkownikom i portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania i zmianę koloru tła.

Wymagania szczegółowe dla systemu zarządzania punktami dostępu do sieci bezprzewodowej – kontrolerów sieci WLAN

Scentralizowane zarządzanie, dla dużej sieci bezprzewodowej, w ramach której realizowane są dodatkowo funkcjonalności lokalizacji, jest jednym z bardziej istotnych elementów infrastruktury sieci bezprzewodowej. Ponadto odpowiednia komunikacja pomiędzy komponentami systemu zarządzania i kontroli dostępu (NAC), pozwala na zwiększenie poziomu bezpieczeństwa sieci, przy jednoczesnym ułatwieniu jej utrzymania. Poniżej przedstawione są wymagania do spełnienia, w celu realizacji odpowiednich funkcjonalności w ramach sieci bezprzewodowej. Należy zwrócić uwagę, że przedstawione wymagania są per kontroler, a zakładana jest jego redundancja – w systemie wysokiej dostępności (instalacja drugiej instancji na osobnym serwerze, w środowisku VMware). Przy czym serwery zakłada się współdzielone w ramach całej infrastruktury IT, dla których wymagania przedstawione są w dalszej części projektu.

Parametry systemu

1. Kontroler sieci bezprzewodowej w momencie dostawy musi obsługiwać minimum 10 punktów dostępowych w normalnym trybie pracy. Kontroler musi umożliwiać rozbudowę do minimum 500 punktów dostępowych w trybie normalnej pracy oraz do minimum 1000 punktów w trybie wysokiej dostępności.
2. Kontroler sieci WLAN musi być dostarczony jako maszyna wirtualna, musi wspierać środowisko co najmniej VMware ESXi.

Mechanizmy przekazywania danych

1. Kontroler musi obsługiwać jednocześnie różne mechanizmy przekazywania danych, w tym routing, tunelowanie ruchu z AP (Bridge@Controller) i zamykanie ruchu w AP (Bridge@AP).
2. Różne mechanizmy przekazywania danych muszą być dostępne do skonfigurowania w podziale na wirtualne grupy sieciowe.

Captive portal

1. Musi posiadać zintegrowany (w kontrolerze), logicznie wydzielony portal dostępowy (Captive Portal), dowolnie konfigurowany przez administratora, z wykorzystaniem wbudowanych narzędzi edycyjnych, wykorzystujących mechanizmy HTML.
2. Dostęp gościnny poprzez Captive Portal musi umożliwiać logowanie do sieci WLAN z wykorzystaniem autentykacji 802.1x.
3. Dostęp gościnny poprzez Captive Portal musi umożliwiać logowanie do sieci WLAN poprzez otrzymanie zezwolenia od uprawnionych użytkowników lub administratora.
4. Captive Portal będzie dawał dostęp Gościom do zasobów sieci Internet w dedykowanej podsieci (Sieć Gości), nie dopuszczając Gości do zasobów wewnętrznych (Intranet).
5. Administrator lub uprawiony użytkownik przydzielając dostęp do Sieci Gości ma mieć wybór przydzielenia dostępu w interwałach czasu.

Zapewnienie jakości w sieci - QoS

1. Musi zapewniać możliwość zmiany parametrów QoS (802.1p, ToS/DSCP i rate-limit) i zmianę list ACL dla dowolnego użytkownika bez zrywania istniejących sesji.
2. Musi obsługiwać przypisywanie indywidualnych parametrów obsługi ruchu poszczególnym użytkownikom (QoS, ACL), bez konieczności segmentacji przez dedykowane SSID.
3. Musi obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence.

Bezpieczeństwo

1. Musi obsługiwać szyfrowanie połączeń do punktów dostępowych sieci WLAN (AP) na poziomie minimum AES 128bit.
2. System musi obsługiwać przypisywanie polityk klientom, bez konieczności segmentacji przez dedykowane SSID.
3. System musi obsługiwać ujednoliconą, opartą na rolach kontrolę dostępu do sieci przewodowej i bezprzewodowej.
4. System musi umożliwiać automatyczną ochronę typu Over The Air Intrusion Prevention przed zagrożeniami takimi jak fałszywe punkty dostępowe, źle skonfigurowane punkty dostępowe, sieci typu ad hoc, spoofing MAC, punkty dostępowe typu Evil Twin lub Honeypot, itp.
5. System musi umożliwiać ochronę przed atakami typu Denial of Service, w tym takimi jak wysyłanie tysięcy fałszywych uwierzytelnień lub asocjacji, „zalewanie" poleceniami unieważnienia uwierzytelnienia lub dysasocjacji, „zalewanie" wiadomościami protokołu EAPOL (EAP over LAN).
6. System musi umożliwiać możliwość lokalizacji zagrożeń, bez względu na to czy są one aktualnie aktywne czy też nie.
7. System musi umożliwiać administratorom sieci zmianę przeznaczenia punktów dostępowych realizujących usługi WLAN na sensory, na stałe lub tymczasowo przez prostą operację zarządzania polegającą na naciśnięciu odpowiedniego przycisku.
8. System powinien umożliwiać wykrywanie access-pointów typu rouge (IEEE 802.11a/g/n/ac).

Zarządzenie

1. Musi umożliwiać zarządzanie poprzez telnet, ssh, https, snmpv3 oraz dedykowaną aplikację do zarządzania.
2. System musi obsługiwać wiele typów kontrolerów (wirtualnych i sprzętowych) dla różnych typów wdrożeń sieci.
3. Wymagane jest scentralizowane raportowanie i konfiguracja WIPS/WIDS.
4. W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie, bez interwencji użytkownika.
5. System zarządzania łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika.
6. Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g oraz 802.11n/ac.
7. System zarządzania łącznością radiową RF Management musi wspierać funkcje automatycznego wyboru kanału i automatycznej kontroli mocy emitowanego sygnału TPC (Transmit Power Control).
8. Kontroler musi zapewniać zarządzanie oparte o graficzny interfejs użytkownika
9. Musi pozwalać nietechnicznym pracownikom na tworzenie tymczasowych kont gości i dystrybuowanie zezwoleń poprzez łatwy w użyciu graficzny interfejs użytkownika

10. Kontroler musi umożliwiać tworzenie raportów NetFlow oraz wysyłanie ich wraz z początkowymi pakietami przepływów do systemu analitycznego pozwalającego monitorować utylizację sieci przez aplikacje.

Integracja z innymi systemami

Musi w pełni współpracować z punktami AP, projektowanym systemem zarządzania oraz rozwiązaniem kontroli dostępu do sieci NAC (systemami przedstawionymi powyżej).

Wymagania szczegółowe dla serwerów na potrzeby instalacji poszczególnych komponentów systemu zarządzania siecią LAN i Security

Serwery na potrzeby niniejszego projektu powinny umożliwiać instalacje poszczególnych komponentów systemów zarządzania, monitorowania i kontroli dostępu do sieci, przewidywane powyżej. Przy czym powinny również zapewniać wstępną konfigurację minimalną, zapewniającą dodatkowo odpowiedni zapas mocy i ilości wolnego miejsca, w celu rozbudowy poszczególnych systemów. Poniżej znajdują się wymagania na poszczególne komponenty, w celu zapewnienia odpowiedniego poziomu działania systemu.

Przedstawiony poniżej serwer do wirtualizacji, może być równoważny, pod warunkiem pełnego wsparcia instalowanych później na nim komponentów oprogramowania zarządzającego, kontrolującego infrastrukturą sieciową.

Konfiguracja podstawowa

1. Obudowa o wysokości 2U, z obsługą procesorów w wersji 4 Intel.
2. Obudowa umożliwiająca wyposażenie do minimum 8 dysków 2,5”.
3. Posiadająca szyny do montażu w szafie serwerowej 19’ i system do zarządzania okablowaniem w tylnej części obudowy.

Procesor

1. Podstawowy processor typu minimum: Intel Xeon E5-2630 v4 2.2GHz,25M Cache,8.0 GT/s QPI,Turbo,HT,10C/20T (85W) Max Mem 2133MH.
2. Dodatkowy/redundanty procesor – jak wyżej, minimum: Intel Xeon E5-2630 v4 2.2GHz 25M Cache 8.0 GT/s QPI Turbo HT 10C/20T (85W) Max Mem 2133MHz.

Szybkość/typ i ilość minimalna pamięci DIMM

1. Zakładany typ pamięci: 2400MT/s RDIMMs.
2. Liczba pamięci min. 4 x 32GB RDIMM, 2400MT/s, Dual Rank, x4 Data Width.

Możliwość wirtualizacji i oprogramowanie do wirtualizacji

1. VMware ESXi 6.5 Embedded Image on Flash Media.
2. vSphere Ess Plus Kit 6CPU License, (subskrypcja, zgodnie z wymaganiami wsparcia technicznego, 3 lata) – zakłada się, pojedynczą licencję oprogramowania obejmującą oba serwery, w celu optymalizacji zarządzania poszczególnymi maszynami wirtualnymi.
3. Oprogramowanie – system operacyjny w zależności od wymagań dla oprogramowania zarządzającego.

Konfiguracja RAID

RAID 5 w oparciu o dedykowany kontroler.

Dyski twarde

Minimum 3 dyski x 2TB 7.2K RPM SATA 6Gbps 512n 2.5in z możliwością wymiany w trakcie pracy.

Zasilacz w postaci redundantnej umożliwiający zabezpieczenie przed awarią

1. Dual, Hot-plug, Redundant Power Supply (1+1).
2. Kable zasilające – 2 zgodnie ze standardem CE.

System do zarządzania serwerem w wersji zaawansowanej, niezależny od systemu operacyjnego dostępny w oparciu o dedykowany interfejs sieciowy.

Karta sieciowa, posiadająca minimum porty

1. 2 porty w standardize 10GBASE-T.
2. 2 porty w standardzie 1GBASE-T.

Wewnętrzny napęd optyczny

Internal DVD+/- RW, SATA

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

Przestawione we wcześniejszej części opisu komponenty sieciowe, zostały przedstawione szczegółowo poniżej, w ramach odpowiednich rozdziałów. Przedstawione zakresy są zakresami minimalnymi do spełnienia, w umożliwienia na etapie realizacji funkcjonalności wymaganych w ramach wdrażanych systemów i aplikacji wykorzystywanych na obiekcie. Przy czym wymagania związane z oprogramowaniem przedstawione są powyżej, w ramach wymaganych funkcjonalności systemu zarządzania. Poniżej znajdują się głównie komponenty sprzętowe, wymagane do zastosowania, przy czym ilości per punkt dystrybucyjny, przedstawione są w wcześniejszej części projektu.

Przełącznik LAN/Security – 48 portowy PoE+ - przełącznik dostępowy w poszczególnych punktach dystrybucyjnych

Przełącznik sieciowy, z jednolitej rodziny przełączników dostępowych zastosowanych i wymaganych w ramach projektu, w celu między innymi ujednolicenia platformy sprzętowej, konfiguracyjnej w ramach infrastruktury sieci, zwiększając poziom elastyczności rozbudowy, jak i jej poziomu utrzymania. Różnice pomiędzy systemami zostały uwzględnione poniżej w specyfikacji (LAN/Security).

Wymagania podstawowe

1. Przełącznik posiadający min. 48 interfejsów 10/100/1000BASE-T, min. 2 interfejsy uplink 10GBASE-X SFP+ oraz 2 interfejsy 10GBASE-X SFP+ do łączenia urządzeń w stos. Przy czym zakresie zakłada się pełną dostępność portów 10GBASE-X (jeżeli jest to z wymaganiem dodatkowej licencji – należy ją uwzględnić w ramach projektu – dla części LAN, dla części Security wykorzystywane porty 1GBase-X).
2. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management.
3. Przełącznik musi wspierać technologię Power over Ethernet (PoE) zgodnie ze standardami IEEE 802.3af (PoE) oraz IEEE 802.3at (PoE+) do zasilania urządzeń takich jak punkty dostępowe WLAN, telefony IP i kamery monitoringu wizyjnego, czy inne systemy.
4. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich interfejsach 10/100/1000BASE-T.
5. Wysokość urządzenia nie więcej niż 1U.
6. Przełącznik musi posiadać wbudowany zasilacz 230V AC zapewniający budżet mocy dla technologii PoE na poziomie min. 740W zapewniając jednocześnie min. 15W dla wszystkich interfejsów 10/100/100BASE-T.

7. Przełącznik musi mieć możliwość instalacji dodatkowego wewnętrznego lub zewnętrznego źródła zasilania.
8. Przełącznik musi posiadać nieblokującą architekturę o wydajności przełączania min. 170 Gb/s oraz szybkości przełączania min. 130 Mp/s.
9. Musi posiadać możliwość realizacji stosów – łączenia fizycznych przełączników w zarządzane zpojedynczego adresu IP jedno logiczne urządzenie. Do łączenia przełączników muszą być wykorzystane dedykowane interfejsy – bez ograniczania liczby interfejsów uplink. Architektura stosu musi umożliwiać realizację zamkniętej pętli. Wydajność przełączania w stosie min. 40Gbps. Wymagana jest możliwość łączenia do 8 przełączników w stos (w tym również przełączników nie wspierających technologii PoE).
10. Tablica MAC adresów min. 16k.
11. Pamięć operacyjna: min. 1GB pamięci DRAM.
12. Pamięć flash: min. 2GB pamięci Flash.
13. Pojemność bufora pakietów min. 1,5 MB.
14. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
15. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
16. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów).
17. Obsługa Q-in-Q IEEE 802.1ad.
18. Obsługa Quality of Service:

- IEEE 802.1p,
- DiffServ,
- 8 kolejek priorytetów na każdym porcie wyjściowym.

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

Obsługa routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.
2. Pojemność tabeli routingu min. 450 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4 ze wsparciem przynajmniej dla protokołu RIPv1/v2.
5. Policy Based Routing dla IPv4.
6. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF.

Obsługa routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.

2. Pojemność tabeli routingu min. 225 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6 ze wsparciem przynajmniej dla protokołu RIPng.
5. Policy Based Routing dla IPv6.
6. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF v3.

Obsługa ruchu multicast

1. Statyczne przyłączenie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa IGMP v1 (RFC 1112).
4. Obsługa IGMP v2 (RFC 2236).
5. Obsługa IGMP v3 (RFC 3376).
6. Obsługa IGMP v1/v2/v3 snooping.

Bezpieczeństwo sieciowe

1. Obsługa uwierzytelniania stacji roboczych z wykorzystaniem mechanizmów:

- IEEE 802.1x,
- Web-based,
- Adres MAC.

2. Obsługa wielu sesji uwierzytelniających (min. 4) na jednym porcie.
3. Przydział sieci VLAN, ACL i parametrów QoS podczas uwierzytelniania.
4. Wsparcie dla profilowania urządzeń podłączających się do przełącznika. Profil 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.

5. Obsługa Guest VLAN.
6. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos.
7. Obsługa TACACS+ (RFC 1492).
8. Obsługa RADIUS Authentication (RFC 2865).
9. Obsługa RADIUS Accounting (RFC 2866).
10. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu (ACL) pracujące na warstwie 2, 3 i 4.
11. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika.
12. Obsługa bezpiecznego transferu plików SCP/SFTP.
13. Obsługa DHCP Option 82.
14. Obsługa Trusted DHCP Server.
15. Obsługa DHCP Snooping.

16. Ograniczanie przepustowości (rate limiting) na interfejsach wyjściowych z kwantem 8 kb/s.
17. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
18. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
19. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
20. Obsługa PVST+.Obsługa G.8032.
21. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – min. 64 grupy po 8 interfejsów.

Zarządzanie

1. Obsługa synchronizacji czasu NTP/SNTP.
2. Zarządzanie przez SNMP v1/v2/v3.
3. Zarządzanie przez przeglądarkę WWW z wykorzystaniem protokołu http i https.
4. Telnet Serwer/Klient dla IPv4 / IPv6.
5. SSH2 Serwer/Klient dla IPv4 / IPv6.
6. Ping dla IPv4 / IPv6.
7. Traceroute dla IPv4 / IPv6.
8. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
9. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757).
10. Obsługa RMON2 (RFC 2021).
11. Obsługa skryptów CLI ze wsparciem funkcji TCL.

Przełącznik LAN/Security – 24 portowy PoE+ - przełącznik dostępowy w poszczególnych punktach dystrybucyjnych

Przełącznik sieciowy, z jednolitej rodziny przełączników dostępowych zastosowanych i wymaganych w ramach projektu, w celu między innymi ujednolicenia platformy sprzętowej, konfiguracyjnej w ramach infrastruktury sieci, zwiększając poziom elastyczności rozbudowy, jak i jej poziomu utrzymania. Różnice pomiędzy systemami zostały uwzględnione poniżej w specyfikacji (LAN/Security).

Wymagania podstawowe

1. Przełącznik posiadający 24 porty 1G 100/1000BASE-T PoE+.
2. Przełącznik posiadający 4 portów 1G SFP (może być w postaci combo z portami 24 portowymi).
3. Przełącznik mający (licencje, dodatkowy moduł) 4 porty 10G SFP+ - dla części LAN, dla Security porty 1GBase-X.
4. Przełącznik musi obsługiwać optykę 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-LRM.
5. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T.
6. Wysokość urządzenia 1U.
7. Przełącznik musi posiadać wbudowany zasilacz 230V AC.
8. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.

9. Nieblokującą architekturę o wydajności przełączania min. 128 Gb/s.
10. Szybkość przełączania min. 95 Milionów pakietów na sekundę.
11. Możliwość łączenia do 8 przełączników w stos.
12. Musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR oraz włókien światłowodowych.
13. Tablica MAC adresów min. 16k.
14. Pamięć operacyjna: min. 1GB pamięci DRAM.
15. Pamięć flash: min. 4GB pamięci Flash.
16. Pojemność bufora pakietów min. 1,5MB.
17. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
18. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
19. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
20. Obsługa Q-in-Q IEEE 802.1ad.
21. Obsługa Quality of Service:

- IEEE 802.1p
- DiffServ
- 8 kolejek priorytetów na każdym porcie wyjściowym

22. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
23. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) .
24. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
25. Wbudowany DHCP serwer i klient.
26. Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
27. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash.
28. Możliwość monitorowania zajętości CPU.
29. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).
30. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.

Obsługa Routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.
2. Pojemność tabeli routingu min. 480 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4:

- RIPv1/v2
- OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania

5. Policy Based Routing dla IPv4.
6. Obsługa DHCP/BootP Relay dla IPv4.

Obsługa Routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.
2. Pojemność tabeli routingu min. 240 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6:

- RIPng
- OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania

5. Obsługa MLDv1 oraz MLDv2 (Multicast Listener Discovery).
6. Policy Based Routing dla IPv6.
7. Obsługa DHCP/BootP Relay dla IPv6.

Obsługa Multicastów

1. Statyczne przyłączenie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa Multicast VLAN Registration – MVR.
4. Obsługa IGMP v1 (RFC 1112).
5. Obsługa IGMP v2 (RFC 2236).
6. Obsługa IGMP v3 (RFC 3376).
7. Obsługa IGMP v1/v2/v3 snooping.

Bezpieczeństwo

1. Obsługa Network Login:

- IEEE 802.1x
- Web-based Network Login
- MAC based Network Login

2. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants).
3. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control).
4. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC.
5. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login.
6. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma.
7. Urządzenie musi wspierać profile bezpieczeństwa, 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.

8. Obsługa Guest VLAN dla IEEE 802.1x.
9. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos.

10. Wbudowana obrona procesora urządzenia przed atakami DoS.
11. Obsługa TACACS+ (RFC 1492).
12. Obsługa RADIUS Authentication (RFC 2865).
13. Obsługa RADIUS Accounting (RFC 2866).
14. RADIUS and TACACS+ per-command Authentication.
15. Bezpieczeństwo MAC adresów:

- ograniczenie liczby MAC adresów na porcie,
- zatrzaśnięcie MAC adresu na porcie,
- możliwość wpisania statycznych MAC adresów na port/vlan.

16. Możliwość wyłączenia MAC learning.
17. Obsługa SNMPv1/v2/v3.
18. Klient SSH2.
19. Zabezpieczenie przełącznika przed atakami DoS:

- Networks Ingress Filtering RFC 2267,
- SYN Attack Protection,
- Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania.

20. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4.
21. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika.
22. Obsługa bezpiecznego transferu plików SCP/SFTP.
23. Obsługa DHCP Option 82.
24. Obsługa Gratuitous ARP Protection.
25. Obsługa Trusted DHCP Server.
26. Obsługa DHCP Snooping.
27. Obsługa DHCP Secured ARP/ARP Validation.
28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s.

Bezpieczeństwo sieciowe

1. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania.
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
5. Obsługa PVST+.
6. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619.
7. Obsługa G.8032.
8. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów.
9. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzenie

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol).
2. Obsługa synchronizacji czasu NTP.
3. Zarządzanie przez SNMP v1/v2/v3.
4. Zarządzanie przez przeglądarkę WWW – protokół http i https.
5. Telnet Serwer/Klient dla IPv4 / IPv6.
6. SSH2 Serwer/Klient dla IPv4 / IPv6.
7. Ping dla IPv4 / IPv6.
8. Traceroute dla IPv4 / IPv6.
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
10. Sprzętowa obsługa sFlow .
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757).
12. Obsługa RMON2 (RFC 2021).
13. Obsługa skryptów CLI ze wsparciem funkcji TCL.

Przełącznik LAN/Security – 48 portowy - przełącznik dostępowy w poszczególnych punktach dystrybucyjnych

Przełącznik sieciowy, z jednolitej rodziny przełączników dostępowych zastosowanych i wymaganych w ramach projektu, w celu między innymi ujednolicenia platformy sprzętowej, konfiguracyjnej w ramach infrastruktury sieci, zwiększając poziom elastyczności rozbudowy, jak i jej poziomu utrzymania. Różnice pomiędzy systemami zostały uwzględnione poniżej w specyfikacji (LAN/Security).

Wymagania podstawowe

1. Przełącznik posiadający 48 portów 1G 10/100/1000BASE-T oraz dodatkowo minimum 2 porty 1/10 Gigabit Ethernet SFP+, z dostępnymi portami 10GBase-X (LAN).
2. Przełącznik musi obsługiwać optykę 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-LRM.
3. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T.
4. Wysokość urządzenia 1U.
5. Przełącznik musi posiadać wbudowany zasilacz 230V AC.
6. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
7. Nieblokującą architekturę o wydajności przełączania min. 175 Gb/s.
8. Szybkość przełączania min. 130 Milionów pakietów na sekundę.
9. Możliwość łączenia do 8 przełączników w stos.
10. Musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR oraz włókien światłowodowych.
11. Tablica MAC adresów min. 16k.
12. Pamięć operacyjna: min. 1GB pamięci DRAM.

13. Pamięć flash: min. 2GB pamięci Flash.
14. Pojemność bufora pakietów min. 1,5 MB.
15. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000.
16. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
17. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
18. Obsługa Q-in-Q IEEE 802.1ad.
19. Obsługa Quality of Service:

- IEEE 802.1p,
- DiffServ,
- 8 kolejek priorytetów na każdym porcie wyjściowym.

20. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
21. Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
22. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
23. Wbudowany DHCP serwer i klient.
24. Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
25. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash.
26. Możliwość monitorowania zajętości CPU.
27. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).
28. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.

Obsługa Routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.
2. Pojemność tabeli routingu min. 450 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4:

- RIPv1/v2,
- OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania.

5. Policy Based Routing dla IPv4.
6. Obsługa DHCP/BootP Relay dla IPv4.

Obsługa Routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.
2. Pojemność tabeli routingu min. 225 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6:

- RIPng,
- OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania.

5. Obsługa MLDv1 (Multicast Listener Discovery version 1).

6. Obsługa MLDv2 (Multicast Listener Discovery version 2).
7. Policy Based Routing dla IPv6.
8. Obsługa DHCP/BootP Relay dla IPv6.
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106.

Obsługa Multicastów

1. Statyczne przyłączenie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa Multicast VLAN Registration – MVR.
4. Obsługa IGMP v1 (RFC 1112).
5. Obsługa IGMP v2 (RFC 2236).
6. Obsługa IGMP v3 (RFC 3376).
7. Obsługa IGMP v1/v2/v3 snooping.

Bezpieczeństwo

1. Obsługa Network Login:

- IEEE 802.1x - RFC 3580,
- Web-based Network Login,
- MAC based Network Login.

2. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants).
3. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control).
4. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC.
5. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login.
6. Urządzenie musi wspierać profile bezpieczeństwa, 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.

7. Obsługa Guest VLAN dla IEEE 802.1x.
8. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos.
9. Wbudowana obrona procesora urządzenia przed atakami DoS.
10. Obsługa TACACS+ (RFC 1492).
11. Obsługa RADIUS Authentication (RFC 2865).
12. Obsługa RADIUS Accounting (RFC 2866).
13. RADIUS and TACACS+ per-command Authentication.
14. Bezpieczeństwo MAC adresów:

- ograniczenie liczby MAC adresów na porcie,
- zatrzaśnięcie MAC adresu na porcie,

- możliwość wpisania statycznych MAC adresów na port/vlan.

15. Możliwość wyłączenia MAC learning.
16. Obsługa SNMPv1/v2/v3.
17. Klient SSH2.
18. Zabezpieczenie przełącznika przed atakami DoS:

- Networks Ingress Filtering RFC 2267,
- SYN Attack Protection,
- Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania.

19. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4.
20. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika.
21. Obsługa bezpiecznego transferu plików SCP/SFTP.
22. Obsługa DHCP Option 82.
23. Obsługa Gratuitous ARP Protection.
24. Obsługa Trusted DHCP Server.
25. Obsługa DHCP Snooping.
26. Obsługa DHCP Secured ARP/ARP Validation.
27. Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x.
28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s.

Bezpieczeństwo sieciowe

1. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania.
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
5. Obsługa PVST+.
6. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619.
7. Obsługa G.8032.
8. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów.
9. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol).
2. Obsługa synchronizacji czasu NTP.
3. Zarządzanie przez SNMP v1/v2/v3.
4. Zarządzanie przez przeglądarkę WWW – protokół http i https.
5. Telnet Serwer/Klient dla IPv4 / IPv6.
6. SSH2 Serwer/Klient dla IPv4 / IPv6.

7. Ping dla IPv4 / IPv6.
8. Traceroute dla IPv4 / IPv6.
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
10. Sprzętowa obsługa sFlow.
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757).
12. Obsługa RMON2 (RFC 2021).

Inne

1. Obsługa skryptów CLI.
2. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych).
3. Możliwość uruchamiania skryptów:

- Ręcznie,
- O określonym czasie lub co wskazany okres czasu,
- Na podstawie wpisów w logu systemowym.

Przełącznik LAN/Security – 24 portowy - przełącznik dostępowy w poszczególnych punktach dystrybucyjnych

Przełącznik sieciowy, z jednolitej rodziny przełączników dostępowych zastosowanych i wymaganych w ramach projektu, w celu między innymi ujednolicenia platformy sprzętowej, konfiguracyjnej w ramach infrastruktury sieci, zwiększając poziom elastyczności rozbudowy, jak i jej poziomu utrzymania. Różnice pomiędzy systemami zostały uwzględnione poniżej w specyfikacji (LAN/Security).

Wymagania podstawowe

1. Przełącznik posiadający:

- 20 portów 1GE 100/1000BASE-T,
- 4 porty 1GE 1000BASE-X SFP,
- 4 porty 10GE 10GBASE-X SFP (LAN, w części Security porty 1GBase-X).

2. Przełącznik musi obsługiwać optykę 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-LRM
3. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T.
4. Wysokość urządzenia 1U.
5. Przełącznik musi posiadać wbudowany zasilacz 230V AC.
6. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację. wewnętrznego lub zewnętrznego dodatkowego zasilacza.
7. Nieblokującą architekturę o wydajności przełączania min. 128 Gb/s.
8. Szybkość przełączania min. 95 Milionów pakietów na sekundę.
9. Możliwość łączenia do 8 przełączników w stos.
10. Musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR oraz włókien światłowodowych.
11. Tablica MAC adresów min. 16k.

12. Pamięć operacyjna: min. 1GB pamięci DRAM.
13. Pamięć flash: min. 4GB pamięci Flash.
14. Pojemność bufora pakietów min. 1,5MB.
15. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
16. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
17. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
18. Obsługa Q-in-Q IEEE 802.1ad.
19. Obsługa Quality of Service:

- IEEE 802.1p,
- DiffServ,
- 8 kolejek priorytetów na każdym porcie wyjściowym.

20. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
21. Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
22. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
23. Wbudowany DHCP serwer i klient.
24. Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
25. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash.
26. Możliwość monitorowania zajętości CPU.
27. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).
28. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.

Obsługa Routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.
2. Pojemność tabeli routingu min. 480 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4:

- RIPv1/v2,
- OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania.

5. Policy Based Routing dla IPv4.
6. Obsługa DHCP/BootP Relay dla IPv4.

Obsługa Routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.
2. Pojemność tabeli routingu min. 240 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6:

- RIPng,
- OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania.

5. Obsługa MLDv1 oraz MLDv2 (Multicast Listener Discovery).
6. Policy Based Routing dla IPv6.
7. Obsługa DHCP/BootP Relay dla IPv6.

Obsługa Multicastów

1. Statyczne przyłączenie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa Multicast VLAN Registration – MVR.
4. Obsługa IGMP v1 (RFC 1112).
5. Obsługa IGMP v2 (RFC 2236).
6. Obsługa IGMP v3 (RFC 3376).
7. Obsługa IGMP v1/v2/v3 snooping .

Bezpieczeństwo

1. Obsługa Network Login

- IEEE 802.1x,
- Web-based Network Login,
- MAC based Network Login.

2. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants).
3. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control).
4. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC.
5. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login.
6. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma.
7. Urządzenie musi wspierać profile bezpieczeństwa, 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.

8. Obsługa Guest VLAN dla IEEE 802.1x.
9. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos.
10. Wbudowana obrona procesora urządzenia przed atakami DoS.
11. Obsługa TACACS+ (RFC 1492).
12. Obsługa RADIUS Authentication (RFC 2865).
13. Obsługa RADIUS Accounting (RFC 2866).
14. RADIUS and TACACS+ per-command Authentication.
15. Bezpieczeństwo MAC adresów:

- ograniczenie liczby MAC adresów na porcie,
- zatrzaśnięcie MAC adresu na porcie,
- możliwość wpisania statycznych MAC adresów na port/vlan.

16. Możliwość wyłączenia MAC learning.
17. Obsługa SNMPv1/v2/v3.
18. Klient SSH2.
19. Zabezpieczenie przełącznika przed atakami DoS:

- Networks Ingress Filtering RFC 2267,
- SYN Attack Protection,
- Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania.

20. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4.
21. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika.
22. Obsługa bezpiecznego transferu plików SCP/SFTP.
23. Obsługa DHCP Option 82.
24. Obsługa Gratuitous ARP Protection.
25. Obsługa Trusted DHCP Server.
26. Obsługa DHCP Snooping.
27. Obsługa DHCP Secured ARP/ARP Validation.
28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s.

Bezpieczeństwo sieciowe

1. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania.
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
5. Obsługa PVST+.
6. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619.
7. Obsługa G.8032.
8. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów.
9. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol).
2. Obsługa synchronizacji czasu NTP.
3. Zarządzanie przez SNMP v1/v2/v3.
4. Zarządzanie przez przeglądarkę WWW – protokół http i https.
5. Telnet Serwer/Klient dla IPv4 / IPv6.
6. SSH2 Serwer/Klient dla IPv4 / IPv6.

7. Ping dla IPv4 / IPv6.
8. Traceroute dla IPv4 / IPv6.
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
10. Sprzętowa obsługa sFlow.
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757).
12. Obsługa RMON2 (RFC 2021).
13. Obsługa skryptów CLI ze wsparciem funkcji TCL.

Przełącznik LAN/Security – 24 portowy - przełącznik dostępowy na potrzeby realizacji światłowodowych

Przełącznik sieciowy, z jednolitej rodziny przełączników dostępowych zastosowanych i wymaganych w ramach projektu, w celu między innymi ujednolicenia platformy sprzętowej, konfiguracyjnej w ramach infrastruktury sieci, zwiększając poziom elastyczności rozbudowy, jak i jej poziomu utrzymania. Przełącznik jest wykorzystywany zarówno w części sieci LAN, jak i na potrzeby podłączenia systemów Security.

Wymagania podstawowe

1. Przełącznik posiadający

- min. 24 interfejsów 1000BASE-X SFP,
- min 4 interfejsy uplink 1000BASE-X SFP,
- min 4 interfejsy 10/100/1000BASE-T RJ45 (dopuszczalne interfejsy combo).

Minimalna liczba jednocześnie wykorzystywanych interfejsów: 28.

2. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management.
3. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich interfejsach 10/100/1000BASE-T.
4. Wysokość urządzenia nie więcej niż 1U.
5. Przełącznik musi posiadać wbudowany zasilacz 230V AC oraz możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego źródła zasilania.
6. Przełącznik musi posiadać nieblokującą architekturę o wydajności przełączania min. 128 Gbps oraz szybkości przełączania min. 95 Mpps.
7. Musi posiadać możliwość realizacji stosów – łączenia fizycznych przełączników w zarządzane z pojedynczego adresu IP jedno logiczne urządzenie. Architektura stosu musi umożliwiać realizację zamkniętej pętli. Wymagana jest możliwość łączenia do 8 przełączników w stos.
8. Tablica MAC adresów min. 16k.
9. Pamięć operacyjna: min. 1GB pamięci DRAM.
10. Pamięć flash: min. 2GB pamięci Flash.
11. Pojemność bufora pakietów min. 1,5 MB.
12. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
13. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
14. Wsparcie dla ramek Jumbo Frames (min. 9198 bajtów).

15. Obsługa Q-in-Q IEEE 802.1ad.
16. Obsługa Quality of Service:

- IEEE 802.1p
- DiffServ
- 8 kolejek priorytetów na każdym porcie wyjściowym

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

Obsługa routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.
2. Pojemność tabeli routingu min. 480 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4 ze wsparciem przynajmniej dla protokołu RIPv1/v2.
5. Policy Based Routing dla IPv4.
6. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF.

Obsługa routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.
2. Pojemność tabeli routingu min. 240 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6 ze wsparciem przynajmniej dla protokołu RIPng.
5. Policy Based Routing dla IPv6.
6. Możliwość licencyjnej rozbudowy rozszerzającej funkcje routingu o protokół OSPF v3.

Obsługa routingu IPv4

1. Statyczne przyłączenie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa IGMP v1 (RFC 1112).
4. Obsługa IGMP v2 (RFC 2236).
5. Obsługa IGMP v3 (RFC 3376).
6. Obsługa IGMP v1/v2/v3 snooping.

Bezpieczeństwo sieciowe

1. Obsługa uwierzytelniania stacji roboczych z wykorzystaniem mechanizmów:

- IEEE 802.1x,
- Web-based,
- Adres MAC.

2. Obsługa wielu sesji uwierzytelniających (min. 4) na jednym porcie.
3. Przydział sieci VLAN, ACL i parametrów QoS podczas uwierzytelniania.
4. Wsparcie dla profilowania urządzeń podłączających się do przełącznika. Profil 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.

5. Obsługa funkcjonalności Guest VLAN.
6. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos.
7. Obsługa TACACS+ (RFC 1492).
8. Obsługa RADIUS Authentication (RFC 2865).
9. Obsługa RADIUS Accounting (RFC 2866).
10. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu (ACL) pracujące na warstwie 2, 3 i 4.
11. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika.
12. Obsługa bezpiecznego transferu plików SCP/SFTP.
13. Obsługa DHCP Option 82.
14. Obsługa Trusted DHCP Server.
15. Obsługa DHCP Snooping.
16. Ograniczanie przepustowości (rate limiting) na interfejsach wyjściowych z kwantem 8 kb/s.
17. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
18. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
19. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
20. Obsługa PVST+.
21. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – min. 64 grupy po 8 interfejsów.

Zarządzanie

1. Obsługa synchronizacji czasu NTP/SNTP.
2. Zarządzanie przez SNMP v1/v2/v3.
3. Zarządzanie przez przeglądarkę WWW z wykorzystaniem protokołu http i https.
4. Telnet Serwer/Klient dla IPv4 / IPv6.
5. SSH2 Serwer/Klient dla IPv4 / IPv6.
6. Ping dla IPv4 / IPv6.

7. Traceroute dla IPv4 / IPv6.
8. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
9. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757).
10. Obsługa RMON2 (RFC 2021).
11. Obsługa skryptów CLI ze wsparciem funkcji TCL.

Przełącznik Security – 12 portowy z PoE+ - przełącznik dostępowy w poszczególnych punktach dystrybucyjnych

Przełącznik sieciowy, z jednolitej rodziny przełączników dostępowych zastosowanych i wymaganych w ramach projektu, w celu między innymi ujednolicenia platformy sprzętowej, konfiguracyjnej w ramach infrastruktury sieci, zwiększając poziom elastyczności rozbudowy, jak i jej poziomu utrzymania.

Wymagania podstawowe

1. Przełącznik posiadający 12 porty 1G 100/1000BASE-T PoE+.
2. Przełącznik posiadający 4 portów 1G SFP.
3. Przełącznik mający możliwość rozbudowy (licencje, dodatkowy moduł) o 4 porty 10G SFP+.
4. Przełącznik musi obsługiwać optykę 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-LRM.
5. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T.
6. Wysokość urządzenia 1U.
7. Przełącznik musi posiadać wbudowany zasilacz 230V AC.
8. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
9. Nieblokującą architekturę o wydajności przełączania min. 104 Gb/s.
10. Szybkość przełączania min. 77 Milionów pakietów na sekundę.
11. Możliwość łączenia do 8 przełączników w stos.
12. Musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR oraz włókien światłowodowych.
13. Tablica MAC adresów min. 16k.
14. Pamięć operacyjna: min. 1GB pamięci DRAM.
15. Pamięć flash: min. 4GB pamięci Flash.
16. Pojemność bufora pakietów min. 1,5MB.
17. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
18. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
19. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
20. Obsługa Q-in-Q IEEE 802.1ad.

21. Obsługa Quality of Service:

- IEEE 802.1p,
- DiffServ,
- 8 kolejek priorytetów na każdym porcie wyjściowym.

22. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
23. Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
24. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
25. Wbudowany DHCP serwer i klient.
26. Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
27. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash.
28. Możliwość monitorowania zajętości CPU.
29. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).
30. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.

Obsługa Routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.
2. Pojemność tabeli routingu min. 480 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4`;

- RIPv1/v2,
- OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania.

5. Policy Based Routing dla IPv4.
6. Obsługa DHCP/BootP Relay dla IPv4.

Obsługa Routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.
2. Pojemność tabeli routingu min. 240 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6.

- RIPng,
- OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania.

5. Obsługa MLDv1 oraz MLDv2 (Multicast Listener Discovery).
6. Policy Based Routing dla IPv6.
7. Obsługa DHCP/BootP Relay dla IPv6.

Obsługa Multicastów

1. Statyczne przyłączenie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa Multicast VLAN Registration – MVR.

4. Obsługa IGMP v1 (RFC 1112).
5. Obsługa IGMP v2 (RFC 2236).
6. Obsługa IGMP v3 (RFC 3376).
7. Obsługa IGMP v1/v2/v3 snooping.

Bezpieczeństwo

1. Obsługa Network Login:

- IEEE 802.1x,
- Web-based Network Login,
- MAC based Network Login.

2. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants).
3. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control).
4. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC.
5. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login.
6. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma.
7. Urządzenie musi wspierać profile bezpieczeństwa, 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.

8. Obsługa Guest VLAN dla IEEE 802.1x.
9. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos.
10. Wbudowana obrona procesora urządzenia przed atakami DoS.
11. Obsługa TACACS+ (RFC 1492).
12. Obsługa RADIUS Authentication (RFC 2865).
13. Obsługa RADIUS Accounting (RFC 2866).
14. RADIUS and TACACS+ per-command Authentication.
15. Bezpieczeństwo MAC adresów:

- ograniczenie liczby MAC adresów na porcie,
- zatrzaśnięcie MAC adresu na porcie,
- możliwość wpisania statycznych MAC adresów na port/vlan.

16. Możliwość wyłączenia MAC learning.
17. Obsługa SNMPv1/v2/v3.
18. Klient SSH2.
19. Zabezpieczenie przełącznika przed atakami DoS:

- Networks Ingress Filtering RFC 2267,

- SYN Attack Protection,
- Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania.

20. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4.
21. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika.
22. Obsługa bezpiecznego transferu plików SCP/SFTP.
23. Obsługa DHCP Option 82.
24. Obsługa Gratuitous ARP Protection.
25. Obsługa Trusted DHCP Server.
26. Obsługa DHCP Snooping.
27. Obsługa DHCP Secured ARP/ARP Validation.
28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s.

Bezpieczeństwo sieciowe

1. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania.
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
5. Obsługa PVST+.
6. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619.
7. Obsługa G.8032.
8. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów.
9. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzenie

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol).
2. Obsługa synchronizacji czasu NTP.
3. Zarządzanie przez SNMP v1/v2/v3.
4. Zarządzanie przez przeglądarkę WWW – protokół http i https.
5. Telnet Serwer/Klient dla IPv4 / IPv6.
6. SSH2 Serwer/Klient dla IPv4 / IPv6.
7. Ping dla IPv4 / IPv6.
8. Traceroute dla IPv4 / IPv6.
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
10. Sprzętowa obsługa sFlow.
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757).
12. Obsługa RMON2 (RFC 2021).

Inne

1. Obsługa skryptów CLI.
2. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych).
3. Możliwość uruchamiania skryptów:

- Ręcznie,
- O określonym czasie lub co wskazany okres czasu,
- Na podstawie wpisów w logu systemowym.

Media konwerter ze standardu 10/100/1000Base-T na 100/Base-X – zarządzalny, na potrzeby realizacji połączeń światłowodowych

Zarządzalny media konwerter światłowodowy powinien zapewniać dualną prędkość przesyłania w oparciu o medium światłowodowe. Zakłada się, że media konwerter powinien pracować w środowisku i warunkach przemysłowych, z możliwością montażu zarówno na szynie DIM, jak i na ścianie. Powinien umożliwiać zarządzanie w oparciu o protokół SNMP. Poniżej przedstawione są szczegółowe wymagania dotyczące konwertera światłowodowego. Zakłada się, że zasilacz może być wspólny zarówno dla konwertera światłowodowego, jak i modułu zasilającego PoE, zapewniającego zasilanie 60W dla urządzeń (kamer) zewnętrznych.

Wymagania podstawowe

1. Konwersja sygnału z 10/100/1000Base-T na 100/1000Base-X.
2. Wsparcie dla 100/100 SFP w zależności od konieczności 100/1000Base-X SFP, w założeniu obsadzony w moduł 1000Base-X, tego samego producenta, co pozostałe moduły.
3. Powinien mieć możliwość podłączenia podwójnego zasilania DC, przy czym zakłada się, że w projekcie zasilanie jest pojedyncze, z możliwością zapewnienia redundancji zasilania w przyszłości.
4. Zgodny ze standardem IP30.
5. Pracujący w rozszerzonych zakresach temperatur: -20 – 75oC.
6. Posiadający certyfikację UL60950-1, CE, FCC, EN50121-4 oraz zgodny z specyfikacjami przemysłowymi: EMS, EMI EN61000-6-2, EN61000-6-4.
7. Posiadający funkcjonalność auto-laser shutdown, w przypadku wykrycia braku sygnału UTP.
8. Posiada wsparcie dla Digital Diagnostic Monitor Interface (DDMI) dla modułów SFP.
9. Zarządzalny jest z poziomu WWW i SNMP.
10. Wspiera do 16 IEEE 802.1Q VLAN Tag.
11. Posiada możliwość wysyłania trapów SNMP w związku z zgubieniem zasilania bądź przejścia portu w tryb down.
12. Posiada zdalny tryb testu z zapętleniem – loop back test.

Specyfikacja

1. Wspiera standardy:

- IEEE802.3 10Base-T,
- 10Mbit/s Ethernet,
- IEEE802.3u 100Base-TX,
- 100Base-FX,
- Fast Ethernet IEEE802.3ab,

- 1000Base-TX Gbit/s Ethernet,
- IEEE802.3z 1000Base-X Gbit/s Ethernet,
- IEEE802.3x Flow Control and Back pressure,
- IEEE802.3ah OAM.

2. Dla portów światłowodowych:

- 100Base-X or 1000Base-X wsparcie dlA Auto Laser Shutdown (ALS),
- wsparcie dla diagnostyki DDMI dla modułów SFP.

3. Dla portów UTP:

- 10/100/1000Base-T Auto MDI/MDI-X z funkcją Auto-Negotiation,
- UTP CAT.5e Twisted Pair,

4. Wspiera ramki typu Jumbo Frames – do 9k.
5. Wspiera:

- Fiber Cable (Multi-mode): 50/125um,62.5/125um,
- Fiber Cable (Single-mode): 9/125um,
- Długość fali: 1310nm (Multi-mode/Single-mode).

6. Na każdym posiada diody: Power 1 (Zielona), Power 2 (Zielona), Fault (Błąd) Fiber LNK/ACT (Zielona).
7. Zakres pracy w temperaturach: -20-75oC.
8. Poziom zasilania: 4.8W.
9. Montaż: na ścianie, bądź na szynie DIM – w założeniu konwerter powinien być dostarczony z możliwością montażu na szynie DIM.
10. Posiada możliwość podłączenia dwóch źródeł zasilania, z możliwością podłączenia systemu alarmowego – 7 PIN-ów.

Gigabitowy Power Injector PoE+ zapewniający zasilanie zgodnie ze standardem IEEE 802.3at/af.15.4/30/36/60W

Moduł zapewniający odpowiedni poziom zasilania dla urządzeń końcowych w oparciu o standard IEE 802.at/af z poziomem mocy do 60W. Zakłada się, że zasilacz może być wspólny zarówno dla konwertera światłowodowego, jak i modułu zasilającego PoE, zapewniającego zasilanie 60W dla urządzeń (kamer) zewnętrznych. Poniżej przedstawione są wymagania zbiorcze dla urządzenia.

Wymagania podstawowe

1. Posiada port podający zasilanie w standardzie 802.3 at/af.
2. W oparciu o ustawienia jest w stanie podać poziom zasilania 15.4W, 30W, 36W, 60W.
3. Pracuje w rozszerzonym zakresie temperatury: -10 – 60oC.
4. Montowany jest na szynie DIM.
5. Wspiera standardy:

- IEEE 802.3 10Base-T Ethernet,
- IEEE 802.3u 100Base-T Fast Ethernet,
- IEEE 802.3ab 1000Base-T Gigabit Ethernet,
- IEEE 802.3at,
- IEEE 802.3af.

6. Poziom poboru mocy: 31,1 W lub 62,8W – na podstawie wymagań wynikających z budżetu mocy.
7. Posiada 2 złącza PIN do podłączenia zasilacza.

Przełącznik spine/warstwa agregująca Security – 48 portów 100/1000BASE-X SFP, 4 1000/10G BASE-X SFP+

Przełącznik warstwy agregującej dla ruchu sieciowego Security, zainstalowany w punkcie dystrybucyjny GPD - serwerownia, połączony z przełącznikiem szkieletowym, w celu wymiany informacji pomiędzy systemami teletechnicznymi (np. BMS, CCTV, kontrola dostępu).

Wymagania podstawowe

1. Przełącznik posiadający 48 portów 1000BASE-X SFP, 4 porty 10GBASE-X SFP+.
2. Wysokość urządzenia 1U.
3. Nieblokująca architektura o wydajności przełączania min. 330 Gb/s.
4. Szybkość przełączania min. 250 Milionów pakietów na sekundę.
5. Możliwość łączenia do 8 przełączników w stos.
6. Tablica MAC adresów min. 98000.
7. Pamięć operacyjna: min. 1GB pamięci DRAM.
8. Pamięć flash: min. 1GB pamięci Flash.
9. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
10. Obsługa sieci wirtualnych protokołowych IEEE 802.1v.
11. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
12. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
13. Obsługa Q-in-Q IEEE 802.1ad.
14. Obsługa Quality of Service:

- IEEE 802.1p,
- DiffServ,
- 8 kolejek priorytetów na każdym porcie wyjściowym.

15. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
16. Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
17. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
18. Przełącznik musi być wyposażony w dwa zasilacze prądu zmiennego, które umożliwiają uzyskanie redundancji zasilania. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika.
19. Przełącznik musi być wyposażony w moduł wentylatorów z możliwością wymiany podczas pracy (hot-swap).
20. Wbudowany DHCP Serwer i klient.
21. Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
22. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash.
23. Możliwość monitorowania zajętości CPU.
24. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).

25. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
26. Wbudowany dodatkowy port Gigabit/ Ethernet do zarządzania poza pasmem - out of band management oraz port szeregowy.
27. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika.

Obsługa Routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.
2. Pojemność tabeli routingu min. 12 tys. wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4:

- RIPv1/v2,
- OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania,
- BGPv4 – możliwość rozszerzenia przez licencję oprogramowania,
- IS-IS – możliwość rozszerzenia przez licencję oprogramowania,

5. Policy Based Routing dla IPv4.
6. Obsługa DHCP/BootP Relay dla IPv4.

Obsługa Routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.
2. Pojemność tabeli routingu min. 6 tys. wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6:

- RIPng,
- OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania,
- BGPv4 – możliwość rozszerzenia przez licencję oprogramowania,
- IS-IS - możliwość rozszerzenia przez licencję oprogramowania,

5. Telnet Serwer/Klient dla IPv6.
6. SSH2 Serwer/Klient dla IPv6.
7. Ping dla IPv6.
8. Tracert dla IPv6.
9. Obsługa 6to4 (RFC 3056).
10. Obsługa MLDv1 (Multicast Listener Discovery version 1).
11. Obsługa MLDv2 (Multicast Listener Discovery version 2).
12. Policy Based Routing dla IPv6.
13. Obsługa DHCP/BootP Relay dla IPv6.
14. Opcja IPv6 Router Advertisement dla DNS - RFC 6106.

Obsługa Multicastów

1. Statyczne przyłączenie do grupy multicast.
2. Filtrowanie IGMP.

3. Obsługa PIM-SM.
4. Obsługa PIM-DM.
5. Obsługa PIM-SSM.
6. Obsługa PIM snooping.
7. Obsługa Multicast VLAN Registration – MVR.
8. Obsługa IGMP v1 (RFC 1112).
9. Obsługa IGMP v2 (RFC 2236).
10. Obsługa IGMP v3 (RFC 3376).
11. Obsługa IGMP v1/v2/v3 snooping.
12. Możliwość konfiguracji statycznych tras dla Routingu Multicastów.

Bezpieczeństwo

1. Obsługa Network Login:

- IEEE 802.1x - RFC 3580,
- Web-based Network Login,
- MAC based Network Login.

2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants).
3. Możliwość integracji funkcjonalności Network Login z Microsoft NAP.
4. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login.
5. Obsługa Guest VLAN dla IEEE 802.1x.
6. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos.
7. Obsługa Identity Management.
8. Wbudowana obrona procesora urządzenia przed atakami DoS.
9. Obsługa TACACS+ (RFC 1492).
10. Obsługa RADIUS Authentication (RFC 2138).
11. Obsługa RADIUS Accounting (RFC 2139).
12. RADIUS and TACACS+ per-command Authentication.
13. Bezpieczeństwo MAC adresów:

- ograniczenie liczby MAC adresów na porcie,
- zatrzaśnięcie MAC adresu na porcie,
- możliwość wpisania statycznych MAC adresów na port/vlan.

14. Możliwość wyłączenia MAC learning.
15. Obsługa SNMPv1/v2/v3.
16. Klient SSH2.
17. Zabezpieczenie przełącznika przed atakami DoS:

- Networks Ingress Filtering RFC 2267,
- SYN Attack Protection,
- Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania,

18. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4:

- Adres MAC źródłowy i docelowy plus maska,
- Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
- Protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.,
- Numery portów źródłowych i docelowych TCP, UDP,
- Zakresy portów źródłowych i docelowych TCP, UDP,
- Identyfikator sieci VLAN – VLAN ID,
- Flagi TCP,
- Obsługa fragmentów.

19. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika.
20. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania.
21. Obsługa bezpiecznego transferu plików SCP/SFTP.
22. Obsługa DHCP Option 82.
23. Obsługa IP Security - Gratuitous ARP Protection.
24. Obsługa IP Security - Trusted DHCP Server.
25. Obsługa IP Security - DHCP Secured ARP/ARP Validation.
26. Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x.
27. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s.

Bezpieczeństwo sieciowe

1. Możliwość konfiguracji portu głównego i zapasowego.
2. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania.
3. Obsługa redundancji routingu VRRP na dwóch urządzeniach agregacyjnych pracujących w ramach MLAG w trybie Active-Active (obydwa urządzenia przeprowadzają routing) - możliwość rozszerzenia przez licencję oprogramowania.
4. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
5. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
6. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
7. Obsługa PVST+.
8. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619.
9. Obsługa G.8032.
10. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów.
11. Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.
12. Obsługa LACP w ramach MLAG.

Zarządzanie

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol).
2. Obsługa synchronizacji czasu NTP.
3. Zarządzanie przez SNMP v1/v2/v3.

4. Zarządzanie przez przeglądarkę WWW – protokół http i https.
5. Możliwość zarządzania poprzez protokół XML.
6. Telnet Serwer/Klient dla IPv4 / IPv6.
7. SSH2 Serwer/Klient dla IPv4 / IPv6.
8. Ping dla IPv4 / IPv6.
9. Traceroute dla IPv4 / IPv6.
10. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757).
12. Obsługa RMON2 (RFC 2021).
13. Obsługa IPFIX.

Inne wymagania

1. Możliwość rozszerzenia funkcjonalności o MPLS poprzez wymianę oprogramowania lub licencję. Wymagane wsparcie dla następujących funkcjonalności: MPLS/VPLS, MPLS/VPWS, LDP, RSVP-TE, Fast Reroute.
2. Obsługa skryptów CLI.
3. Obsługa skryptów języka Python.
4. Wsparcie OpenFlow – możliwość rozszerzenia przez licencję oprogramowania.
5. Obsługa AVB (Audio Video Bridging) – możliwość rozszerzenia przez licencję oprogramowania
6. Obsługa funkcji TCL/Tk w skryptach CLI.
7. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych).
8. Możliwość uruchamiania skryptów:

- Ręcznie,
- O określonym czasie lub co wskazany okres czasu,
- Na podstawie wpisów w logu systemowym.

<u>Przełącznik spine/warstwa szkieletowa sieci LAN – 48 portów 1/10GBASE-X SFP+, 4 40G BASE-X QSFP+</u>

Przełączniki warstwy szkieletowej stanowią jeden z najważniejszych komponentów projektowanej sieci LAN, ze względu na zbieranie ruchu sieciowego z poszczególnych przełączników dostępowych, umożliwiając jednocześnie na odpowiednią separację ruchu sieciowego. Odpowiednio zaprojektowany szkielet sieci, wraz z odpowiednimi funkcjonalnościami umożliwia na realizację nie tylko wysokowydajnej sieci LAN, umożliwiającej wdrożenie odpowiednich mechanizmów niezawodności i bezpieczeństwa, ale również elastyczność rozbudowy, w przypadku konieczności, choćby zwiększenia wydajności sieci, ze względu na wprowadzane nowe usługi sieciowe. Jednocześnie jednolitość platformy konfiguracji systemu operacyjnego, ułatwia utrzymanie odpowiedniego poziomu jakości sieci LAN, jednolitej konfiguracji i polityki bezpieczeństwa sieci, a co za tym idzie również utrzymania w przyszłości. Poniżej przedstawione wymagania dotyczą pojedynczego przełącznika szkieletowego.

Wymagania podstawowe

1. Przełącznik posiadający 48 portów 10Gigabit Ethernet SFP+, mogących pracować z prędkością 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+ oraz 4 porty 40G z interfejsami QSFP+.
2. Możliwość użycia portów 40G w trybie 4 x 10G.
3. Wysokość urządzenia 1U.
4. Nieblokująca architektura o wydajności przełączania min. 1250 Gb/s .
5. Szybkość przełączania min. 950 Milionów pakietów na sekundę.
6. Przełącznik musi posiadać zainstalowane dwa zasilacze, które umożliwiają uzyskanie redundancji zasilania. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika.
7. Chłodzenie przód-tył.
8. Tablica MAC adresów min. 128k.
9. Pamięć operacyjna: min. 1 GB pamięci DRAM.
10. Pamięć flash: min. 1 GB pamięci Flash.
11. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
12. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
13. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
14. Obsługa Q-in-Q IEEE 802.1ad.
15. Obsługa Quality of Service:

- IEEE 802.1p,
- DiffServ/DSCP,
- 8 kolejek priorytetów na każdym porcie wyjściowym.

16. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
17. Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
18. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
19. Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
20. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash.
21. Możliwość monitorowania zajętości CPU.
22. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).
23. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
24. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
25. Wbudowany port konsoli RS-232.

Obsługa Routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.

2. Pojemność tabeli routingu min. 16 tys. wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4:

- RIP v1/v2,
- OSPFv2 - możliwość rozszerzenia przez licencje,
- BGPv4 - możliwość rozszerzenia przez licencje,
- IS-IS - możliwość rozszerzenia przez licencje.

5. Policy Based Routing dla IPv4.
6. Obsługa DHCP/BootP Relay dla IPv4.

Obsługa Routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.
2. Pojemność tabeli routingu min. 8 tys. wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6:

- RIPng,
- OSPF v3 – możliwość rozszerzenia przez licencje,
- BGPv4 – możliwość rozszerzenia przez licencje,
- IS-IS – możliwość rozszerzenia przez licencje.

5. Ping dla IPv6.
6. Tracert dla IPv6.
7. Obsługa 6to4 (RFC 3056).
8. Obsługa MLDv1 (Multicast Listener Discovery version 1).
9. Obsługua MLDv2 (Multicast Listener Discovery version 2).
10. Policy Based Routing dla IPv6.
11. Obsługa DHCP/BootP Relay dla IPv6.
12. Opcja IPv6 Router Advertisement dla DNS - RFC 6106.

Obsługa Multicastów

1. Statyczne przyłączanie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa PIM-SM.
4. Obsługa PIM-DM.
5. Obsługa PIM-SSM.
6. Obsługa PIM snooping.
7. Obsługa Multicast VLAN Registration – MVR.
8. Obsługa IGMP v1 - RFC 1112.
9. Obsługa IGMP v2 - RFC 2236.
10. Obsługa IGMP v3 - RFC 3376.
11. Obsługa IGMP v1/v2/v3 snooping.
12. Możliwość konfiguracji statycznych tras dla Routingu Multicastów.

Bezpieczeństwo

1. Kontrola dostępu do sieci:

- IEEE 802.1x - RFC 3580,
- Autentykacja MAC.

2. Kontrola dostępu wielu klientów na jednym porcie (Multidomain Authentication).
3. Możliwość integracji z systemem kontroli dostępu do sieci (NAC – Network Access Control).
4. Przydział sieci VLAN, ACL, ograniecznie pasma podczas logowania do sieci.
5. Obsługa TACACS+.
6. Obsługa RADIUS Authentication (RFC 2138).
7. Obsługa RADIUS Accounting (RFC 2139).
8. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4:

- Adres MAC źródłowy i docelowy plus maska,
- Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6,
- Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.,
- Numery portów źródłowych i docelowych TCP, UDP,
- Zakresy portów źródłowych i docelowych TCP, UDP,
- Identyfikator sieci VLAN - VLAN ID,
- Flagi TCP,
- Obsługa fragmentów.

9. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika.
10. Możliwość zliczania pakietów trafiających do ACL.
11. Obsługa transferu plików TFTP/SCP.
12. Obsługa DHCP Option 82.
13. Gratuitous ARP Protection.
14. Trusted DHCP Server.
15. DHCP Snooping.
16. Dynamic ARP Inspection.
17. Ograniczanie przepustowości (rate limiting) na portach wyjściowych.

Bezpieczeństwo sieciowe

1. Obsługa redundancji routingu VRRP - RFC 2338.
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
5. Obsługa PVST+.
6. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 64 grupy po 8 portów.
7. Obsługa Multichassis EtherChannel.

Zarządzanie

1. Obsługa synchronizacji czasu NTP.

2. Zarządzanie przez SNMP v1/v2/v3.
3. Zarządzanie przez przeglądarkę WWW – protokół http i https.
4. Możliwość zarządzania przez protokół XML.
5. Telnet Serwer/Klient dla IPv4 / IPv6.
6. SSH2 Serwer/Klient dla IPv4 / IPv6.
7. Ping dla IPv4 / IPv6.
8. Traceroute dla IPv4 / IPv6.
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
10. Sprzętowa obsługa NetFlow lub sFlow.
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events.

Inne wymagania

1. Obsługa Data Center Bridging.
2. Obsługa Priority Flow Control (PFC).
3. Obsługa Enhanced Transmission Selection (ETS).
4. Obsługa OpenFlow – możliwość rozszerzenia przez licencje lub wymianę oprogramowania.
5. Obsługa skryptów CLI.
6. Obsługa funkcji TCL w skryptach CLI.
7. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych).
8. Możliwość uruchamiania skryptów:

- Ręcznie,
- O określonym czasie lub co wskazany okres czasu,
- Na podstawie wpisów w logu systemowym.

Przełącznik do warstwy serwerowej sieci LAN – 48 portów 1/10GBASE-T, 4 10G/40G BASE-X QSFP, 2 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28

Warstwa dostępu do sieci poszczególnych serwerów, odpowiednio wydajna, jednocześnie elastyczna w swojej architekturze, z możliwością rozbudowy, przy zapewnieniu jednocześnie odpowiedniego poziomu bezpieczeństwa, jest kluczowa dla funkcjonowania systemów i aplikacji wykorzystywanych, zarówno na początku działania sieci w Szpitalu, jak i później w trakcie realizacji dodatkowych, tymczasowych wystaw i innych konferencji lub imprez masowych. Poniżej zostały przedstawione wymagania projektowanego systemu ToR, dostępu do sieci dla poszczególnych serwerów, z zapewnieniem odpowiedniego poziomu wydajności i bezpieczeństwa.

Wymagania podstawowe

1. Przełącznik posiadający 48 portów 1Gb/10Gb 10GBASE-T, 4 porty 10Gb/40Gb QSFP+ oraz 2 porty 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28.
2. Dedykowany port do zarządzania przełącznikiem poza pasmem.
3. Dedykowany port konsoli szeregowej RJ-45.
4. Wysokość urządzenia nie większa niż 1U.

5. Możliwość łączenia do 8 urządzeń w stos zarządzany z pojedynczego adresu IP, połączenie pomiędzy urządzeniami musi być możliwe z wykorzystaniem portów 100Gb.
6. Nieblokująca architektura o wydajności przełączania min. 1,7 Tb/s.
7. Przełącznik musi być wyposażony w dwa zasilacze, które umożliwiają uzyskanie redundancji zasilania z możliwością wymiany w czasie działania przełącznika. Zasilacze muszę zapewniać przepływ powietrza przód-tył.
8. Modularny system chłodzenia z przepływem powietrza przód-tył.
9. Tablica MAC adresów min. 270K.
10. Pamięć operacyjna: min. 8 GB RAM DDR3.
11. Pamięć SSD: min. 32 GB.
12. Bufor pakietów: min 12 MB.
13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4092.
14. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
15. Obsługa VxLAN Tunneling End Point (VTEP).
16. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
17. Obsługa Q-in-Q IEEE 802.1ad.
18. Obsługa Quality of Service:

- IEEE 802.1p,
- DiffServ/DSCP.
- 8 kolejek priorytetów na każdym porcie wyjściowym.

19. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
20. Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
21. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
22. Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
23. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci urządzenia.
24. Możliwość monitorowania zajętości CPU.
25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).
26. Obsługa wirtualnych routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.

Obsługa routingu IPv4

1. Sprzętowa obsługa routingu IPv4 – forwarding.
2. Pojemność tabeli routingu min. 260 tys. wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4:

- RIP v1/v2,
- OSPFv2 (dla min. 4 aktywnych interfejsów),

5. Możliwość rozbudowy funkcji routingu IPv4 o protokoły:

- BGP4 oraz MBGP (BGP4+),
- IS-IS,

6. Policy Based Routing dla IPv4.
7. Obsługa DHCP/BootP Relay dla IPv4.

Obsługa routingu IPv6

1. Sprzętowa obsługa routingu IPv6 – forwarding.
2. Pojemność tabeli routingu min. 130 tys. wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6:

- RIPng,
- OSPF v3 (dla min. 4 aktywnych interfejsów).

5. Możliwość rozbudowy funkcji routingu IPv4 o protokoły:

- BGP4 oraz MBGP (BGP4+),
- IS-IS.

6. Ping dla IPv6.
7. Tracert dla IPv6.
8. Obsługa 6to4 (RFC 3056).
9. Obsługa MLDv1 (Multicast Listener Discovery version 1).
10. Obsługua MLDv2 (Multicast Listener Discovery version 2).
11. Policy Based Routing dla IPv6.
12. Obsługa DHCP/BootP Relay dla IPv6.
13. Opcja IPv6 Router Advertisement dla DNS - RFC 6106.

Obsługa multicastów

1. Statyczne przyłączanie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa PIM snooping.
4. Obsługa Multicast VLAN Registration – MVR.
5. Obsługa IGMP v1 - RFC 1112.
6. Obsługa IGMP v2 - RFC 2236.
7. Obsługa IGMP v3 - RFC 3376.
8. Obsługa IGMP v1/v2/v3 snooping.
9. Możliwość konfiguracji statycznych tras dla routingu multicastów.

Bezpieczeństwo

1. Kontrola dostępu do sieci:

- IEEE 802.1x - RFC 3580,
- Autentykacja MAC.

2. Kontrola dostępu wielu klientów na jednym porcie.
3. Możliwość integracji z systemem kontroli dostępu do sieci (NAC – Network Access Control).

4. Przydział sieci VLAN, ACL, ograniczanie pasma podczas logowania do sieci.
5. Obsługa TACACS+.
6. Obsługa RADIUS Authentication (RFC 2138).
7. Obsługa RADIUS Accounting (RFC 2139).
8. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4:

- Adres MAC źródłowy i docelowy plus maska,
- Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6,
- Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.,
- Numery portów źródłowych i docelowych TCP, UDP,
- Zakresy portów źródłowych i docelowych TCP, UDP,
- Identyfikator sieci VLAN - VLAN ID,
- Flagi TCP,
- Obsługa fragmentów.

9. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika.
10. Możliwość zliczania pakietów trafiających do ACL.
11. Obsługa transferu plików TFTP/SCP.
12. Obsługa DHCP Option 82.
13. Gratuitous ARP Protection.
14. Trusted DHCP Server.
15. DHCP Snooping.
16. Dynamic ARP Inspection.
17. Ograniczanie przepustowości (rate limiting) na portach wyjściowych.

Bezpieczeństwo sieciowe

1. Obsługa redundancji routingu VRRP - RFC 2338.
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
5. Obsługa PVST+.
6. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 64 grupy po 8 portów.
7. Obsługa Multichassis EtherChannel.

Zarządzanie

1. Obsługa synchronizacji czasu NTP.
2. Zarządzanie przez SNMP v1/v2/v3.
3. Zarządzanie przez przeglądarkę WWW – protokół http i https.
4. Możliwość zarządzania przez protokół XML.
5. Telnet Serwer/Klient dla IPv4 / IPv6.
6. SSH2 Serwer/Klient dla IPv4 / IPv6.
7. Ping dla IPv4 / IPv6.

8. Traceroute dla IPv4 / IPv6.
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
10. Sprzętowa obsługa NetFlow lub sFlow.
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events.

Inne wymagania

1. Obsługa Data Center Bridging:

- Data Center Bridging Exchange Protocol (DCBx),
- Priority Flow Control (PFC),
- Enhanced Transmission Selection (ETS),

2. Obsługa skryptów CLI:

- Obsługa funkcji TCL w skryptach CLI,
- Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych),
- Możliwość uruchamiania skryptów ręcznie, o określonym czasie lub co wskazany okres czasu oraz na podstawie wpisów w logu systemowym.

Bezprzewodowy punkt dostępu do sieci – Access Point pracujący w standardzie 802.11b/g/n/ac/ac wave2 - podstawowy

Odpowiedni dobór i ich instalacja na etapie wdrożenia urządzeń mających na celu zapewnienie dostęp do sieci bezprzewodowej dla poszczególnych urządzeń końcowych, z odpowiednia jakością dla różnych aplikacji i systemów, wraz z opcją lokalizacji ich, przy jednoczesnym zapewnieniu jednolitej platformy zarządzania całą infrastrukturą, ma ogromne znaczenie dla poprawnego działania sieci komputerowej. Przy czym w przypadku dostępu bezprzewodowego, czyli medium otwartego, bardzo ważne znaczenie ma również zapewnienie bezpieczeństwa sieci, kontrola dostępu, jak i monitorowanie, bądź nawet zwalczanie nieautoryzowanych prób montażu innych urządzeń o podobnym profilu. Poniżej znajdują się wymagania związane z poszczególnymi punktami AP, z uwzględnieniem centralnego zarządzania z wykorzystaniem opisanego wcześniej kontrolera sieci bezprzewodowej, pracującego w trybie niezawodnościowym.

Rozmieszczenie Access Pointów pokazana w załączniku oraz na planie gniazd LAN. Dodatkowo należy przewidzieć montaż AP w dwóch największych windach transportowych. W tym celu należy uzgodnić sposób podłączenia oraz montażu z dostawcą wind.

Pasma robocze

1. Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości:

- 802.11ac/a/n (5 GHz),
- i 802.11b/g/n (2,4 GHz).

2. Poza modułami radiowymi WLAN punkt dostępowy powinien być wyposażony w trzeci moduł radiowy pracujący w paśmie 2,4 GHz służący do obsługi standardów BLE i IEEE 802.15.4.

Interfejsy fizyczne

1. 1 port 10/100/1000 Base-T RJ-45 z technologią autosensing.
2. Port konsolowy RJ-45.

Anteny

1. Musi posiadać min. 5 anten wewnętrznych.

Tryby pracy

1. Tryb działania radio WLAN: Client access, Local mesh, Packet capture, WDS.
2. Możliwość pracy punktu dostępowego bez kontrolera WLAN na wypadek awarii łącza.
3. Obsługa technologii 802.11ac i praca w technice transmisji wieloantenowej MIMO 2x2 przy zasilaniu przez jedno źródło zgodne ze standardem IEEE 802.3af, bez wpływu na działanie kluczowych funkcji i wydajność.
4. Wsparcie dla mechanizmu minimum „Two spatial stream MIMO" dla wszystkich nadajników.
5. WDS (Wireless Distribution System) z możliwością tworzenia łączy typu backhaul na dowolnym łączu radiowym lub wykorzystania jednego łącza radiowego zarówno na potrzeby backhaul, jak i świadczenia usług klientom.
6. Instalacja typu plug & play.
7. Jednoczesna obsługa ruchu tunelowanego i mostowanego.
8. Wszystkie punkty dostępowe muszą mieć możliwość pracy w formie sensorów sieci – pracujących w pełnym lub niepełnym wymiarze czasu.
9. W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie i bez interwencji użytkownika.

Funkcje zarządzania

1. Punkt dostępowy musi zapewniać rozproszone zarządzanie łącznością radiową RF (Radio Frequency) Management niezależne od kontrolera - poza tylko wstępną konfiguracją. Po utracie połączenia z kontrolerem, punkt dostępowy musi być zdolny do zapewnienia ciągłości operacji związanych z szyfrowaniem, tworzeniem czarnych list, filtrowaniem, QoS oraz zarządzaniem łącznością radiową, zarówno dla swoich potrzeb, jak i lokalnie mostowanego ruchu.
2. Zarządzanie łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika.
3. Możliwość konfiguracji zapewniającej równoważenie obciążenia i sterowanie pasmem w celu pozwolenia punktom dostępowym na równoważenie/sterowanie ruchem klientów pomiędzy obiema częstotliwościami na jednym punkcie dostępowym i/lub pomiędzy wieloma punktami dostępowymi w ramach domeny łączności radiowej,
4. Punkty dostępowe muszą mieć możliwość wdrożenia w konfiguracji kratowej, tworzącej bezprzewodowe, wzajemne połączenia pomiędzy poszczególnymi punktami dostępowymi.
5. Możliwość stworzenia i jednoczesnego uruchomienia minimum 16 profili sieci bezprzewodowych WLAN.
6. Każdy profil sieci bezprzewodowej powinien posiadać możliwość przypisania do innej lub tej samej sieci VLAN.
7. Punkty dostępowe muszą umożliwiać generowanie raportów IPFIX oraz wysyłanie ich wraz z początkowymi pakietami przepływów (osobno lub w ramach ruchu IPFIX) do systemu analitycznego pozwalającego monitorować utylizację sieci przez aplikacje.

Standardy sieciowe

Punkt dostępowy musi obsługiwać następujące funkcjonalności:

1. Zgodność z DFS2 (Dynamic Frequency Selection) by dopuścić dodatkowe kanały w paśmie 5 GHz,
2. Punkty dostępowe muszą obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence.
3. Obsługa protokołu 802.11e, w tym WMM oraz U-APSD.
4. Szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC).
5. Obsługa do 16 SSID (8 na częstotliwość radiową).
6. Obsługa minimum 460 użytkowników jednocześnie.
7. RADIUS Authentication & Accounting.
8. Płynny roaming pomiędzy podsieciami IP.
9. Płynny roaming pomiędzy wieloma kontrolerami.
10. Wsparcie dla protokołu IEEE 802.1p prioritization.
11. Możliwość wykonania minimum 24 jednoczesnych połączeń VoIP w ramach protokołu IEEE 802.11 a/b/g/n.
12. Wsparcie dla protokołu: IEEE 802.1X z wykorzystaniem metod: EAP-SIM, EAPFAST, EAP-TLS, EAP-TTLS, and PEAP.
13. Wsparcie dla protokołu: MAC address authentication przy wykorzystaniu lokalnych access-list lub przesyłanych z serwera RADIUS.
14. Mechanizmy: RADIUS AAA, przy wykorzystaniu EAP-MD5, PAP, CHAP oraz MS-CHAPv2.
15. RADIUS Client.
16. Mechanizm izolacji klientów na poziomie L2.
17. Mechanizmy IEEE 802.11i, WPA2 oraz WPA, przy zastosowaniu algorytmów szyfracji: Advanced Encryption Standard (AES) oraz Temporal Key Integrity Protocol (TKIP).
18. Obsługa technologii 802.11ac pracując w konfiguracji 2x2 MIMO.
19. Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g, 802.11n oraz 802.11ac/ac wave2.

Bezpieczeństwo

1. Połączenie pomiędzy AP, a kontrolerem musi być szyfrowane przy pomocy technologii AES minimum 128 bit.
2. Obsługa standardów uwierzytelniania i szyfrowania, w tym: WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x.
3. Możliwość pracy w architekturze bezpieczeństwa opartej na rolach, zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, aplikowane względem zarówno użytkownika, jak i aplikacji, z której korzysta użytkownik.
4. Funkcje egzekwowania przypisanych ról i ograniczania przepustowości muszą być osiągalne na poziomie punktu dostępowego.
5. Przypisywanie ról klientom musi odbywać się bez konieczności segmentacji przez dedykowane SSID.

6. Musi zapewniać wsparcie dla protokołu: MAC address authentication przy wykorzystaniu lokalnych access-list lub przesyłanych z serwera RADIUS.
7. Musi obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń, zgodnie z protokołem CAPWAP RFC 5415 lub równoważnym.
8. Musi mieć możliwość wdrożenia w konfiguracji kratowej, tworzącej bezprzewodowe, wzajemne połączenia pomiędzy poszczególnymi punktami dostępowymi.
9. Obsługa mechanizmów QoS - shaping ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik.
10. Definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID.

Integracja z pozostałymi komponentami sieci

1. Musi umożliwiać wykrywanie lokalizacji systemów końcowych w czasie rzeczywistym i przechowywanie tych informacji w centralnej bazie danych do wykorzystania w procesie implementacji technologii NAC, która jest również przedmiotem postępowania.
2. Musi w pełni współpracować z systemem zarządzania oraz rozwiązaniem kontroli dostępu do sieci NAC.

Inne wymagania

1. Wraz z punktem dostępowym należy dostarczyć, pochodzący od tego samego producenta, co dostarczane urządzenia, uchwyt umożliwiający montaż punktu dostępowego pod sufitem.
2. W związku z charakterystyką urządzeń medycznych znajdujących się w bezpośrednim sąsiedztwie punktów dostępowych muszą one pracować zgodnie ze standardem medycznych urządzeń elektrycznych opisanych certyfikatem zgodności EN 60601-1-2.

<u>Urządzenie w celu zapewnienia funkcjonalności NGFW w ramach sieci wewnętrznej jak i do podłączenia do sieci Internet czy sieci zewnętrznych</u>

System zabezpieczeń sieciowych, jest jednym z kluczowych elementów kompleksowego, projektowanego systemu zabezpieczeń, w warstwie sieciowej i aplikacyjnej w ramach infrastruktury IT. Ma na celu nie tylko odpowiednią separację poszczególnych środowisk i systemów teletechnicznych, od ruchu użytkowników, ale również wychwycenie potencjalnych zagrożeń i zwiększenie poziomu bezpieczeństwa w ramach zintegrowanej infrastruktury sieciowej. Jednocześnie stanowi bardzo ważne ogniwo na styku z siecią Internet, czy systemami/sieciami zewnętrznymi, które będą podłączane do sieci Szpitala, w przyszłości. Poniżej zostały przedstawione podstawowe wymagania do spełnienia przez projektowane rozwiązanie.

Wymagania ogólne

1. System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance).
2. System zabezpieczeń firewall musi zapewniać wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym.
3. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
4. System zabezpieczeń firewall musi umożliwiać działanie w następujących trybach pracy:

- routera (tzn. w warstwie 3 modelu OSI),
- przełącznika (tzn. w warstwie 2 modelu OSI),
- w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA)
- w trybie pasywnego nasłuchu (sniffer).

5. Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.).

6. System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.

7. System zabezpieczeń firewall musi umożliwiać pracę w modelu wysokiej dostępności poprzez pracę dwóch urządzeń w modelu failover. Wymagana jest praca firewalli w modelach Active-Standby i Active-Active.

8. System zabezpieczeń firewall musi umożliwiać licencyjną rozbudowę/obsługiwać nie mniej niż 6 wirtualnych firewalli/systemów/domen/kontekstów, przy czym w ramach dopstawy należy przewidzieć licencję na 2 konteksty. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:

- tablic routingu przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.
- Polityk bezpieczeństwa obejmujących:
    - System IPS,
    - System ochrony antymalware/antyspyware,
    - System ochrony antywirus.
- Koncentratorów VPN dla zdalnego dostępu.

Wymagania dot. platformy, wymagania wydajnościowe

1. System zabezpieczeń firewall musi być wyposażony w co najmniej:

- 8 portów Gigabit Ethernet 1000BASE-T,
- 8 portów Gigabit Ethernet SFP.
- 2 porty 10Gigabit Ethernet SFP+.

2. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.

3. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 4 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji,

4. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 2 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering)

5. System zabezpieczeń firewall musi obsługiwać nie mniej niż 500 000 jednoczesnych połączeń.

Podstawowe wymagania funkcjonalne

1. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
2. Polityka zabezpieczeń firewall musi uwzględniać:

- strefy bezpieczeństwa,
- adresy IP klientów i serwerów,
- protokoły i usługi sieciowe,
- aplikacje,
- kategorie URL,
- użytkowników aplikacji,
- reakcje zabezpieczeń,
- rejestrowanie zdarzeń i alarmowanie,
- zarządzanie pasmem w sieci w oparciu o:
    - priorytet,
    - pasmo gwarantowane,
    - pasmo maksymalne,
    - oznaczenia DiffServ.

3. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
4. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
5. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych.
6. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Kontrola aplikacji musi być przeprowadzana w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.
7. System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
8. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
9. System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antymalware, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

10. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
11. System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
12. System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
13. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
14. System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
15. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

Wymagania dotyczące identyfikacji użytkowników

1. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci
2. System zabezpieczeń firewall musi zapewniać integrację z:

- Active Directory,
- Ms Exchange,
- Citrix,
- LDAP,
- serwerami Terminal Services.

3. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
4. System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w system zabezpieczeń firewall, który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników.
5. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy

analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

Wymagania dotyczące warstwy sieci

1. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
2. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
3. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
4. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
5. System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.
6. System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów.

- Polityki definiujące powinny umożliwiać wykorzystanie
    - adresów źródłowych,
    - adresów docelowych,
    - użytkowników,
    - numerów portów usług
    - kategorie URL.
- System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia
    - RADIUS,
    - TACACS+,
    - LDAP,
    - Kerberos,
    - SAML 2.0.

7. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
8. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
9. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

Wymagania dotyczące zaawansowanych systemów ochrony

1. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.
2. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
3. System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
4. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
5. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
6. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). __
7. System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
8. System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
9. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
10. System zabezpieczeń firewall musi posiadać moduł antymalware lub antyspyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
11. System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja antymalware lub antyspyware uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).

12. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur antymalware lub antyspyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
13. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
14. System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
15. System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
16. System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
17. System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
18. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
19. System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
20. Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
21. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box".
22. System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.

Wymagania dotyczące zarządzania

1. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.

2. System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
3. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
4. System zabezpieczeń firewall musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst witrualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualny nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmianw pojedynczym systemie/kontekście wpływalo w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. W innych systemach wirtualnych
5. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
6. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
7. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
8. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
9. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
10. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 120 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie dopuszcza się aby do tego celu konieczny był zakup zewnętrznych urządzeń, oprogramowania ani licencji.
11. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
12. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
13. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
14. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
15. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
16. System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:

- ruchu sieciowym,
- aplikacjach,
- zagrożeniach
- filtrowaniu stron www.

17. System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
18. System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
19. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

Wsparcie techniczne dla poszczególnych komponentów infrastruktury sieciowej, systemów zarządzania, kontroli i zwiększenia poziomu bezpieczeństwa sieci

Wymagane wsparcie techniczne na poszczególne produkty, wymaga obsługi na wszystkie komponenty sieciowe, systemy zarzadzania przez okres 3 lat od daty dostawy sprzętu i oprogramowania. Dodatkowy okres powinien być możliwy do dostarczenia, opcjonalnie.

W ramach obsługi wsparcia technicznego zakłada się następujące parametry dla urządzeń szkieletowych, agregacyjnych, systemów zarządzania, systemów NAC, systemów zarządzania siecią bezprzewodową, serwerów, urządzeń zapewniających zasilanie PoE+ (za wyjątkiem media konwerterów światłowodowych i urządzeń typu Power Injector):

1. Obsługa w okresie 3 lat w trybie NBD (ang. Next Business Day), świadczone przez producenta danego komponentu sieciowego.
2. Dostępna obsługa TAC (ang. Technical Assistance Center) świadczone przez producenta, dla wszystkich dostarczanych komponentów sieciowych i systemów zarządzania, realizowana w trybie 8x5xNBD.
3. W ramach obsługi serwisowej zapewniony jest dostęp do nowych wersji oprogramowania dla poszczególnych produktów, aktualizacji poszczególnych funkcjonalności i do dokumentacji technicznej przez cały okres świadczenia usług wsparcia technicznego.
4. Wymiana uszkodzonego sprzętu odbywać się przez wymagany okres czasu w trybie NBD.
5. Dla systemów i oprogramowania wymagającego subskrypcji, zakłada się okres 3 lat świadczenie usługi aktualizacji, dostępnej dla poszczególnych systemów, realizowanej bezpośrednio przez producenta.
6. W ramach wsparcia technicznego zapewniony jest bezpośredni dostęp pracowników Szpitala, do wsparcia technicznego producenta danego komponentu sieciowego, systemu zarządzania itp.

Dla pozostałych urządzeń wsparcie techniczne, zakłada się, ze powinno być na poziomie gwarancji LLW (ang. Limited Lifetime Warranty), z świadczeniem serwisu przez okres 3 lat minimum. W ramach gwarancji dostępne dla klienta powinno być: wymiana urządzenia w przypadku awarii w ciągu 10 dni roboczych od daty zgłoszenia, jak i dostępność aktualizacji oprogramowania, w przypadku zaistnienia błędów krytycznych w oprogramowaniu.

Rezerwowanie danych

Na potrzeby rezerwowego zapisu danych, Inwestor zapewni we własnym zakresie rezerwowanie danych na zewnętrznych serwerach.

4.1.3.2 Opis systemu telefonii IP

Założenia ogólne

Zaprojektowany system telefonii IP powinien stanowić nowoczesną i elastyczną platformę dla Szpitala realizująca funkcje zunifikowanej komunikacji dla każdego z użytkowników bez kompromisów, zwiększając efektywność komunikacji i oszczędzając ich czas. System powinien pracować w oparciu o zaprojektowana zunifikowaną infrastrukturę telekomunikacyjną – sieć komputerową LAN i WLAN, z zachowaniem odpowiedniej jakości usług w sieci i połączęń (ang. Quality of Service).

System powinien zapewniać jednolitą (w tym pochodzącą od jednego producenta, bądź w pełni zintegrowaną) platformę komunikacyjną między terminalami audio oraz wideo, zarówno osobistymi jak i dedykowanymi do sal konferencyjnych, czy w przyszłości do sal operacyjnych a także urządzeniami mobilnymi. Dzięki integracji z sieciami telefonii tradycyjnej PSTN i sieciami telefonii komórkowej system powinien dawać możliwość wykorzystania urządzeń mobilnych razem z telefonami i terminalami zainstalowanymi w obrębie sieci wewnętrznej. Platforma powinna jednocześnie zapewniać funkcję „jednego numeru" umożliwiającą przenoszenie rozmowy z sieci komórkowej do systemu telefonii IP i z powrotem, do połączenia mobilnego.

Poniżej zostały przedstawione założenia ogólne wymagane od dostarczanego i zaprojektowanego systemu telefonicznego:

1. System telefonii IP powinien być zbudowany w oparciu o platformę serwerową, składającą się z dwóch serwerów, montowanych w szafie rackowej, na których w postaci zwirtualizowanej działać będą poszczególne wymagane aplikacje funkcjonalne, wymagane do realizacji w ramach kompleksowego systemu telefonii IP dla Szpitala.

2. Poszczególne serwery powinny być dostarczone z licencją do obsługi minimum 520 telefonów i urządzeń końcowych podłączanych do systemu, przy czym sumaryczne minimalne parametry dla systemu dla poszczególnych serwerów to obsługa minimum:

- 1 000 użytkowników systemu telefonicznego,
- 1 200 urządzeń końcowych, aparatów telefonicznych itp.
- 100 agentów pracujących do obsługi centrum kontaktowego z klientami,
- 1 000 skrzynek poczty głosowej.

3. Serwery powinny stanowić system niezawodnościowy (klaster active/passive), dla wybranych aplikacji i systemów dostarczanych w ramach rozwiązania, w celu zachowania ciągłości działania systemu w przypadku awarii.

4. System do realizacji połączeń telefonicznych, tworzenia i zarządzania użytkownikami i końcówkami (telefonami IP), powinien składać się z dwóch aplikacji uruchomionych na osobnych serwerach, pracujących w klastrze niezawodnościowym, z uwzględnieniem hierarchii działania (serwer zarządzający, do tworzenia polityk i serwer do realizacji połączeń głosowych).

5. System telefonii IP powinien współpracować z 2 bramami głosowymi do sieci telefonicznej PSTN, które będą dołączone poprzez interfejsy głosowe ISDN, jak i łącze typu SIP trunk. Bramy głosowe powinny posiadać funkcjonalność SBC (ang. Session Border Controller) dla łączy SIP trunk oraz H.323, w celu podłączenia operatorów PSTN do Szpitala.

6. Bramy głosowe powinny być dostarczone z odpowiednimi modułami obsługującymi:

- 2 x 2 porty typu ISDN E1,
- 2 x 30 sesji do obsługi /terminowania sesji poprzez łącze LAN/WAN (np. SIP).

7. System powinien być dostarczony z bramami głosowymi pochodzącymi od jednego producenta, zapewniając jednocześnie pełną integrację pomiędzy systemami, jak

również gwarancję obsługi, uaktualnień itp. w trakcie trwania umowy wsparcia technicznego dla całego systemu.

8. System powinien być dostarczony z funkcjonalnością do obsługi komunikatora aplikacyjnego, instalowanego na platformy Windows, Mac OS, czy Android, IOS. Komunikator powinien umożliwiać zarządzanie kontaktami, realizować funkcję czatu i wymianę informacji o obecności oraz umożliwiać sterowanie telefonem IP, w ramach wymaganej ilości licencji - wstępnie w ramach dostawy do 35 użytkowników.
9. System powinien zawierać aplikację do wspomagania zarządzania poszczególnymi licencjami i procesem utrzymania systemów i aplikacji, zainstalowanych na poszczególnych serwerach, w ramach pojedynczego systemu.
10. System powinien realizować funkcjonalność zapowiedzi głosowej, z uwzględnieniem funkcjonalności podstawowej contact center, w postaci zapewniającej zintegrowaną platformę IVR – zapowiedzi głosowych, jak również integracji z pocztą e-mail, web chat czy wspomnianego powyżej komunikatora. Zakłada się, że w ramach dostawy system powinien posiadać licencję 5 stanowisk dla agentów contact center.
11. System powinien być wyposażony w serwer faksowy, zintegrowany z systemem telefonii IP, z licencją do obsługi 8 kanałów cyfrowych, faksowych.
12. System komunikacyjny powinien obejmować wszystkie wymagane licencje dla aplikacji, systemów operacyjnych oraz licencji użytkowników, umożliwiające obsługę terminali i funkcjonalności użytkowników w poniższych ilościach:

- 300 użytkowników telefonów IP uproszczonych,
- 200 użytkowników telefonów IP podstawowych (licencja zawiera zapas na potrzeby dołożenia aparatów telefonicznych o funkcjonalności podstawowej),
- 10 użytkowników telefonów IP rozszerzonych,
- 10 użytkowników telefonów IP zaawansowanych wyposażonych w przystawkę,
- 8 użytkowników telefonów IP wideo,
- 2 użytkowników terminali osobistych IP wideo,
- 5 użytkowników dysponującymi aplikacjami do wsparcia obsługi sekretarskiej,
- 35 licencji użytkownika dysponującego dowolnymi komunikatorami podstawowymi (na PC/Windows, MacOS lub mobilnymi), z możliwością wykorzystania dla dowolnego podłączanego urządzenia (użytkownik może korzystać z telefonu jak i komunikatora jednocześnie),
- 5 licencji zapewniających obsługę jednocześnie 5 agentów Contact Center dla usług helpdesku,
- 8 licencji na równoczesne kanały faksowe w systemie serwera faksów IP.

13. System powinien obsługiwać zestaw dla 5 stanowisk operatorskich/sekretarskich, z zintegrowaną aplikacją na komputerze, do przełączania rozmów telefonicznych.
14. System powinien posiadać pojedynczy zestaw do realizacji telekonferencji na salę konferencyjną, wraz z dodatkowymi mikrofonami połączonymi przewodowo.

Poniżej w tabeli zostały przedstawione zbiorczo ogólne wymagania na funkcjonalności poszczególnych komponentów systemu telefonii IP, wraz z wymaganymi ilościami.

lp	Typ/rodzaj komponentu systemu	Ilość	Liczba obsadzonych połączeń sieciowych per urządzenie	Inne wymagania (ogólnie)
1	Serwer z silnikiem wirtualizacyjnym, na którym instalowane są poszczególne komponenty systemu	2	4 x 10GBASE-T	Serwery powinny umożliwiać instalację do 5 systemów do realizacji funkcjonalności telefonii i innych, w zależności od konieczności spełnienia określonych funkcjonalności telefonicznych, wideokonferencyjnych, contact center itp. Serwery powinny posiadać komponenty redundantne, jak zasilacze, podłączenie do sieci LAN. Jednocześnie powinny posiadać silnik wirtualizacyjny, pozwalający na instalację modułów funkcjonalnych (systemów).
2	Scentralizowany system do zarządzania telefonami, połączeniami telefonicznymi, instalowany w postaci maszyny wirtualnej	2	Z uwzględnieniem podłączenia systemu głównego	System powinien zostać zbudowany w oparciu o klaster niezawodnościowy, pracujący jako system nadrzędny (system do tworzenia konfiguracji), system do zapewnienia i obsługi komunikacji (system podrzędny).
3	Wymagane licencje w systemie, dostępne dla poszczególnych rodzajów systemów i aplikacji	300 użytkowników telefonów IP uproszczonych 200 użytkowników telefonów IP podstawowych (licencja zawiera zapas na potrzeby dołożenia aparatów telefonicznych o funkcjonalności podstawowej) 10 użytkowników telefonów IP rozszerzonych 10 użytkowników telefonów IP zaawansowanych wyposażonych w przystawkę 8 użytkowników telefonów IP wideo 2 użytkowników terminali osobistych IP wideo 5 użytkowników dysponującymi aplikacjami do wsparcia obsługi sekretarskiej 35 licencji użytkownika dysponującego dowolnymi komunikatorami podstawowymi (na PC/Windows, MacOS lub mobilnymi), z możliwością wykorzystania dla dowolnego podłączanego urządzenia (użytkownik może korzystać z telefonu jak i komunikatora jednocześnie) 5 licencji zapewniających obsługę jednocześnie 5 agentów Contact Center dla usług helpdesku 8 licencji na równoczesne kanały faksowe w systemie serwera faksów IP		
4	Brama głosowa – realizująca styk z sieciami zewnętrznymi – połączenia cyfrowe ISDN E1	2	2 x ISDN E1 Voice 30 sesji po IP (SIP/H.323) poprzez port LAN /WAN	System do realizacji funkcjonalności komunikacji pomiędzy szpitalem i systemami zewnętrznymi telefonicznymi, w oparciu o połączenia cyfrowe ISDN. Brama głosowa powinna być w pełni zintegrowana z systemem telefonii IP, zapewniając połączenie ISDN i SIP do operatora PSTN.
6	System do realizacji funkcjonalności fax serwera	1	8 kanałów jednocześnie	System zintegrowany z systemem głównym oraz bramą głosową, do obsługi połączeń faksowych w oparciu o połączenia cyfrowe.
7	System rozbudowany sekretarski – w postaci rozbudowanej aplikacji sekretarskiej	1	5 stanowisk	System zintegrowany z dostarczanymi zestawami telefonów, w celu obsługi przekierowania połączeń telefonicznych w oparciu o aplikację na stacjach komputerowych operatorów. Zapewniający obsługę dla 5 stanowisk.
8	System do zarządzania licencjami, dla serwerów pracujących w ramach rozwiązania	1	Pojedynczy na klaster serwerów	System do centralnego zarządzania, scentralizowanej kontroli aplikacji, ich aktualizacji.
9	Telefony IP, w wersji uproszczonej –EC1	269	1 x 10/100Base-T	Uproszczony telefon z możliwością montażu na ścianie. Obsługujący pojedynczą linię telefoniczną.
10	Telefon IP, w wersji podstawowej – EC2 (punkty pielęgniarskie)	17	1 x 10/100Base-T z funkcją przełącznika	Telefon podstawowy z dwoma klawiszami programowalnymi. Obsługa dwóch linii telefonicznych.
11	Terminal wideo IP - dotykowy wideotelefon – EC3	1	1x10/100/1000Base-T	System zunifikowanej komunikacji, zaawansowany, z funkcjonalnością realizacji połączeń zarówno telefonicznych, jak i wideo.
12	Telefon rozszerzony, monochromatyczny z klawiszami szybkiego wybierania numerów – EC4 (sekretarki)	16	1x10/100/1000Base-T	Telefon z możliwością programowania 16 linii/klawiszy szybkiego wybierania, z monochromatycznym wyświetlaczem.
13	Telefon zaawansowany z kolorowym wyświetlaczem z modułem klawiszy programowalnych, szybkiego wybierania – EC5 (informacja)	2	1x10/100/1000Base-T	Telefon z kolorowym wyświetlaczem i modułem rozszerzeń – klawiszy programowalnych, przy czym zakłada się, że system dostarczany jest z obsługą do 36 programowalnych klawiszy.
14	Telefon IP wideo z kolorowym wyświetlaczem – EC6	16	1x10/100/1000Base-T	Telefon z obsługą połączeń telefonicznych i wideo, z możliwością podłączenia identycznego zestawu programowalnych klawiszy szybkiego wybierania, jak w zestawach powyżej.

lp	Typ/rodzaj komponentu systemu	Ilość	Liczba obsadzonych połączeń sieciowych per urządzenie	Inne wymagania (ogólnie)
15	Telefon IP telekonferencyjny – EC7 (sala konferencyjna 5.044)	1	1x10/100Base-T	Telefon IP dedykowany do realizacji telekonferencji, wraz z dwoma dodatkowymi mikrofonami przewodowymi.

Wymagania szczegółowe dla serwerów – platformy sprzętowej na potrzeby instalacji poszczególnych aplikacji i systemów telefonii IP

Serwery na potrzeby niniejszego projektu powinny umożliwiać instalacje poszczególnych komponentów systemów telefonii IP i aplikacji, przewidywane powyżej. Przy czym powinny również zapewniać wstępną konfigurację minimalną, zapewniającą dodatkowo odpowiedni zapas mocy i ilości wolnego miejsca, w celu rozbudowy poszczególnych systemów. Poniżej znajdują się wymagania na poszczególne komponenty, w celu zapewnienia odpowiedniego poziomu działania systemu.

Przedstawiony poniżej serwer do wirtualizacji, może być równoważny, pod warunkiem pełnego wsparcia instalowanych później na nim komponentów oprogramowania zarządzającego, kontrolującego infrastrukturą sieciową. Serwer powinien pochodzić od producenta poszczególnych komponentów telefonii IP, w celu zachowania pełnej kompatybilności i odpowiedzialności producenta za kompleksowy system.

Skalowalność i architektura systemu zunifikowanej komunikacji

1. Rozwiązanie musi mieć pracować w modelu redundancji, to znaczy posiadać zdublowane serwery obsługi połączeń (Call Control) dedykowane do obsługi abonentów.
2. Platforma sprzętowa powinna umożliwiać dalsze skalowanie systemu bez konieczności rozbudowy sprzętowej do poziomu co najmniej 1 000 użytkowników systemu dysponujących łącznie co najmniej 1 200 terminalami IP.
3. System powinien być oparty o platformę zwirtualizowaną umożliwiającą kreowanie maszyn wirtualnych dla poszczególnych komponentów aplikacyjnych na platformie serwerowej.
4. Należy dostarczyć dwa serwery o jednakowej konfiguracji, na obydwu będzie pracować system zarządzania połączeniami. Platforma sprzętowa każdego z dwóch serwerów musi spełniać poniższe parametry minimalne:

- 6 dysków HDD 300GB 6Gb SAS 10K RPM SFF hot plug,
- Kontroler modularny RAID 0/1/5/6, 12G SAS, 1GB FBWC,
- Zdublowany zestaw wentylatorów w układzie chłodzącym serwera,
- Zasilanie AC 230V, hot-swap, możliwość rozbudowy serwera o drugi zasilacz,
- Dwa gniazda CPU,
- Procesor CPU 8-rdzeniowy, 2.4 GHz, 20MB Cache. Typ Intel E5-2630 v3 lub równoważny,
- 32GB pamięci RAM w postaci dwóch układów 16GB DDR4 2133MHz RDIMM/PC4.

5. Obudowa przystosowana do montażu w szafie rack. Serwer powinien posiadać akcesoria do montażu w szafie, wysokość serwera nie może przekraczać 1RU.
6. Wirtualizacja systemu zunifikowanej komunikacji powinna być wspierana przez producenta rozwiązania pod względem technicznym.
7. Należy dostarczyć licencje na wirtualizatory dla serwerów.
8. W celu integracji z inną infrastrukturą serwerową, platforma wirtualizacyjna serwerów komunikacyjnych powinna mieć możliwość rozbudowy do opcji centralnego zarządzania

przez system zarządzania środowiskiem zwirtualizowanym np. VMWare vCenter lub równoważny.

Wymagania szczegółowe dla bram głosowych – platformy sprzętowej na potrzeby instalacji komunikacji do operatorów zewnętrznych PSTN

System do realizacji funkcjonalności bramy głosowej powinien zapewniać możliwość podłączenia do sieci komputerowej w Szpitalu w dowolnym miejscu, w którym dostępna będzie zarówno sieć LAN Szpitala, jak i łącza operatora telekomunikacyjnego PSTN.

Poniżej znajdują się wymagani szczegółowe do spełnienia dla poszczególnych bram głosowych:

1. Brama głosowa musi być urządzeniem pełniącym rolę wielousługowego routera modularnego gotowego do obsługi ruchu głosowego w sieci głosowej PSTN oraz transmisji danych w sieci LAN i WAN (w zależności od możliwości późniejszej realizacji łączy od operatorów telekomunikacyjnych).
2. Brama głosowa musi pozwalać na instalację co najmniej:

- 2 kart sieciowych z interfejsami z możliwością wyłączenia modułu w celu oszczędności energii,
- 1 wewnętrznego modułu DSP z możliwością wyłączenia modułu w celu oszczędności energii,
- Brama głosowa musi posiadać wbudowaną zintegrowaną sprzętową akceleracje szyfrowania DES/3DES/AES do wykorzystania w przyszłości.

3. Brama głosowa musi posiadać możliwość bezpośredniej komunikacji pomiędzy modułami z pominięciem głównego procesora, jeśli ruch sieciowy nie jest skierowany do routera.
4. Musi posiadać wszystkie interfejsy „aktywne”. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
5. Sloty urządzenia przewidziane pod rozbudowę muszą mieć możliwość obsadzenia modułami:

- z cyfrowymi interfejsem T1/E1 dla ruchu głosowego lub ruchu typu channelized z gęstością interfejsów nie mniejszą niż 4 portów T1/E1,
- z interfejsami szeregowymi WAN, w liczbie min. 4 porty na moduł,
- interfejsów głosowych analogowych (FSX/FXO) z gęstością minimum 4 porty FXO lub 4 porty FXS na moduł,
- z dyskiem twardym SSD,
- przełącznika Ethernet (funkcje L2 i L3), oczekiwana liczba portów przełącznika nie może być mniejsza niż 8 dla jednego modułu. Porty przełącznika muszą być dostępne również w wersji z zasilaniem PoE,
- umożliwiającym komunikację po sieci komórkowej w technologii 3G/4G (LTE),
- z portem VDSL2 / ADSL2+ over POTS,
- z portem VDSL2 / ADSL2+ over POTS / Annex M,
- portem VDSL2 / ADSL2+ over ISDN.
- z układami DSP.

6. Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP muszą mieć możliwość obsadzenia modułami:

- gęstości nie mniejszej niż 256 kanałów,
- Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (osługa interfejsów głosowych, trancoding, conferencing) z granulacją do 1 DSP,

- Posiadających wsparcie dla usług wideo,
- Obsługującymi kodeki głosowe:
    - G.711,
    - ClearChannel,
    - G.729a,
    - G.729ab,
    - G.726,
    - G.722,
    - G.728,
    - G.729,
    - G.729b,
    - Internet Low Bit.
- Funkcjonalność FaxRelay,
- Funkcjonalność ModemRelay,
- Obsługującymi funkcjonalność transkodowania pomiędzy różnymi typami kodeków,
- Obsługującymi funkcjonalność konferencji głosowych (musi być możliwość obsłużenia do co najmniej 6 konferencji po 64 uczestników lub 66 konferencji po 8 uczestników),
- Obsługującymi kompresję, wykrywanie aktywności głosowej, zarządzenie jitterem i funkcje kasowanie echa (co najmniej 128 ms). Funkcja kasowania echa musi być zgodna ze standardem ITU-T G.168,
- Szyfrowanie transmisji głosu z wykorzystaniem sRTP,
- Szyfrowanie sygnalizacji z wykorzystaniem TLS.

7. Brama głosowa musi oferować dla pakietów o długości 64bajtów wydajność co najmniej 100 000pps przy zapewnieniu przepustowości rzędu 50Mbps.
8. Brama głosowa musi oferować dla pakietów o długości 64bajtów maksymalną wydajność szyfrowania na poziomie 65 000pps przy zapewnieniu przepustowości rzędu 35Mbps.
9. Musi być zarządzalne za pomocą SNMPv3.
10. Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow/JPFlow lub równoważnego.
11. Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI) jak również interfejsu graficznego (GUI).
12. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
13. Obudowa musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
14. Obudowa musi mieć możliwość montażu w szafie 19” i musi zostać dostarczone z umożliwiającym to zestawem montażowym.
15. Brama głosowa musi mieć możliwość zasilania ze źródeł zmiennoprądowych 230V (zasilacz AC).
16. Brama głosowa musi posiadać wbudowany lub zewnętrzny zasilacz umożliwiający zasilanie prądem przemiennym 230V.
17. Brama głosowa musi umożliwiać doprowadzenie zasilania do portów Ethernet (tzw. inline-power) - w modułach sieciowych dostępnych do urządzenia

18. Brama głosowa musi być wyposażone w minimum 2 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN/WAN, oba interfejsy muszą być wbudowane w urządzenie
19. Minimum jeden z interfejsów opisanych powyżej musi mieć możliwość pracy w trybie „dual-physical" z portem RJ45 lub gigabitowym portem światłowodowym definiowanym przez moduł GBIC lub SFP.
20. Brama głosowa musi być wyposażona w dwa porty ISDN E1 PRA oraz układy DSP do obsługi co najmniej 60 kanałów głosowych.
21. Brama głosowa musi posiadać udokumentowaną współpracę z systemem zarządzania połączeniami.
22. Musi obsługiwać protokół MGCP dla zdalnego sterowania sygnalizacją ISDN Q.931 jej portów głosowych ISDN E1 PRA przez system zarządzania połączeniami w systemie komunikacyjnym.
23. Musi obsługiwać protokoły głosowe SIP oraz H.323.
24. Brama głosowa musi być wyposażona w funkcjonalność kontrolera brzegowego SBC dla protokołu SIP i H.323 dla co najmniej 30 jednoczesnych połączeń głosowych z możliwością rozbudowy do co najmniej 100 sesji SIP i H.323 bez wymiany sprzętu.
25. Urządzenie musi być wyposażone w minimum 4GB pamięci Flash z możliwością rozbudowy do 8GB.
26. Urządzenie musi być wyposażone w minimum 4GB pamięci RAM z możliwością rozbudowy do 8GB.
27. Urządzenie musi być wyposażone w minimum jeden port USB. Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych oraz pełnić funkcję konsoli szeregowej.

<u>Wymagania szczegółowe dla systemu telefonicznego – centralnego systemu do obsługi komponentów telefonii oraz połączeń telefonicznych</u>

Centralny system do realizacji połączeń telefonicznych powinien być dostarczony w wersji zwirtualizowanej, instalowanej na platformie sprzętowej przedstawionej powyżej. System nie powinien wymagać dodatkowej licencji na korzystanie instalowanie poszczególnych jego instancji, do wydajności platformy sprzętowej. Dopuszczana licencja związana powinna być wyłącznie z ilością i jakością obsługiwanych urządzeń końcowych, czy użytkowników systemu telefonii IP. Platforma powinna być w pełni zintegrowana z pozostałymi komponentami infrastruktury telefonii IP, wymaganymi do dostarczenia w ramach niniejszego projektu.

Platforma systemu powinna zapewniać realizację w klastrze niezawodnościowym, w celu zabezpieczenia przed wystąpieniem pojedynczej awarii. Klaster, zakłada, że może pracować w trybie active/active, z rozdzieleniem ról w ramach kompleksowego systemu (zarządzanie użytkownikami, połączeniami itp.). Przy czym w przypadku awarii umożliwia pełne przejęcie funkcjonalności systemu telefonii przez drugi z komponentów.

Podstawowe cele i charakterystyka systemu zunifikowanej komunikacji:

1. System musi realizować zadania zwiększające efektywność komunikacji:

- połączenia głosowe oraz wideo wysokiej jakości z wykorzystaniem kodeków szerokopasmowych,
- obsługa konferencji głosowych, w tym połączeń wielostronnych.

2. Obsługa połączeń wideo, w tym połączeń wielostronnych z zastosowaniem mostków wideo

3. Informowanie o aktualnym stanie dostępności innych użytkowników systemu (dostępny/niedostępny/proszę-nie-przeszkadzać) na terminalu sprzętowym oraz komunikatorze programowym.
4. Dostarczenie interfejsu użytkownika umożliwiającego łatwy dostęp do informacji o nieodebranych/odebranych/wykonanych połączeniach, do poczty głosowej, a także tworzenie własnych książek adresowych.
5. Obniżenie kosztów zarządzania i utrzymania systemu telekomunikacyjnego poprzez

- zdalne zarządzanie całym systemem,
- łatwe i szybkie dokonywanie zmian typu instalacja nowych terminali, zmiana ich parametrów, przenoszenie ich na nowe miejsca pracy,
- wykorzystanie mini-przełącznika wbudowanego w terminal do podłączenia komputerów do sieci LAN (współdzielenie łącza przez komputer i terminal) celem obniżenia kosztów budowy struktury sieci LAN (mniej portów na przełącznikach LAN).

6. Zwiększenie efektywności pracy poprzez:

- większą mobilność i dostępność użytkowników przez umożliwienie im logowania się do systemu z dowolnego terminalu nim objętego,
- możliwość dostępu z poziomu terminalu do informacji pochodzących z różnorodnych aplikacji merytorycznych,
- możliwość zdefiniowania dla użytkownika pojedynczego numeru urzędowego, obejmującego osobisty terminal użytkownika w systemie oraz jego inne urządzenie komunikacyjne spoza niego (np. telefon komórkowy),
- obsługa terminali bezprzewodowych.

7. Bezpieczeństwo komunikacji.
8. Możliwość szyfrowania połączeń.
9. Możliwość identyfikacji urządzeń za pomocą certyfikatów.

Funkcje zarządzania połączeniami w systemie zunifikowanej komunikacji

1. Funkcjonalność systemu zunifikowanej komunikacji w zakresie obsługi połączeń i terminali w zakresie telefonii oraz wideo musi obejmować:

- zestawianie połączeń w oparciu o zdefiniowany plan numeracji,
- możliwość odrzucenia połączeń,
- możliwość warunkowego przekazania połączeń, gdy abonent rozmawia albo nie odbiera połączenia, albo też bezwarunkowo wszystkich połączeń,
- parkowanie połączeń,
- funkcjonalność CallPickup,
- obsługa połączeń oczekujących,
- identyfikacja połączeń przychodzących,
- dostęp do książki telefonicznej bezpośrednio z ekranu terminala. Książka telefoniczna musi mieć możliwość automatycznego uaktualniania z katalogu LDAP,
- obsługa klawiszy szybkiego wybierania numerów,
- podgląd stanu innych linii/numerów,
- możliwość transferowania połączeń,
- oddzwanianie (Callback),
- funkcje grup huntingowych z kolejkowaniem połączeń oraz odtwarzaniem dla połączeń oczekujących zapowiedzi powitalnej i zapowiedzi w trakcie oczekiwania,
- realizacja audiokonferencji aranżowanych w trybach ad-hoc (rozumianym jako: wydzwanianie kolejno do osób, które mają uczestniczyć w konferencji i kolejne dołączanie ich do niej) i meet-me (rozumianym jako: samodzielne wdzwonienie się osób, które mają uczestniczyć w konferencji na podany wcześniej numer), z możliwością udziału w nich łącznie nie mniej niż 128 stron konferencji w jednej lub wielu konferencjach,

- możliwość realizacji wideokonferencji HD720p AVC poprzez współpracę z mostkami wideokonferencyjnymi zarządzanymi z systemu sterowania połączeniami, w celu realizacji konferencji wideo w trybie ad-hoc oraz meet-me. Funkcja mostków wideokonferencyjnych powinny być realizowane na bazie mostków sprzętowych lub programowych. Dostawa mostków nie jest wymagana,
- funkcjonalność sekretarsko-dyrektorską, w tym monitorowanie linii dyrektora przez sekretariat, ograniczanie połączeń do dyrektora, możliwość włączenia przez dyrektora statusu „nie przeszkadzać" oraz funkcję interkom,
- logowanie abonenta na komunikatorze lub telefonie IP, z zachowaniem profilu zalogowanego abonenta (numery linii, uprawnienia abonenckie, ustawienia obsługi połączeń).

2. Funkcjonalność oprogramowania w zakresie zarządzania połączeniami musi obejmować:

- ograniczanie możliwości połączeń (restrykcje), w tym z wymaganiem podania kodu dostępu,
- możliwość generowania raportów połączeń Call Detail Recorts (CDR), zawierających co najmniej informacje statystyczne o numerach abonentów wywołującego i wywoływanego, o czasie rozpoczęcia i zakończenia połączenia – dla celów późniejszego tworzenia zestawień wykorzystania systemu telekomunikacyjnego przez jego użytkowników,
- możliwość generowania raportów połączeń Call Detail Recorts (CDR), zawierających co najmniej informacje diagnostyczne o jakości połączenia (rodzaj kodeka, liczba wysłanych, odebranych i zgubionych pakietów z próbkami głosowymi, zmienność opóźnienia przesyłania tych pakietów a także wyliczona informacja o jakości podawana w postaci uniwersalnej wartości MOS – Mean Opinion Score lub równoważnej), dla celów monitorowania przez administratorów realizacji transmisji głosu w systemie telekomunikacyjnym z właściwą jakością,
- możliwość zalogowania się użytkownika na innym terminalu w systemie, co oznacza czasowe przyjęcie na nim ustawień danego użytkownika (np. jego indywidualnych uprawnień do wykonywania połączeń telefonicznych),
- możliwość zdefiniowania pojedynczego numeru biznesowego na stacjonarnym terminalu użytkownika, którego wywołanie przez połączenie przychodzące z wnętrza systemu lub z zewnątrz (z sieci PSTN) spowoduje automatyczne jednoczesne propagowanie tego połączenia na inne zdefiniowane przez użytkowane numery urządzeń mobilnych (nie mniej niż cztery). Po odebraniu takiego połączenia na którymkolwiek z nich musi być możliwe przenoszenie połączenia pomiędzy urządzeniem mobilnym a terminalem użytkownika bez konieczności przerywania połączenia,
- logiczne przypisanie do wielu terminali jednego i tego samego numeru (np. do terminala stacjonarnego i terminala bezprzewodowego),
- narzędzia do centralnej konfiguracji i zarządzania systemem dla administratora, dostępne poprzez przeglądarkę www,
- narzędzia zarządzania dla użytkowników końcowych dostępne przez przeglądarkę internetową, dające im możliwość konfiguracji podstawowych parametrów ich terminala, zrealizowane w języku polskim.

3. Funkcjonalność systemu zarządzania połączeniami musi zawierać:

- wybór sposobu kompresji głosu dla połączenia - obsługa co najmniej standardów:
    - G.711, G.729 – dla zachowania zgodności systemu telekomunikacyjnego ze starszymi typami telefonów IP oraz zapewnienia możliwości współpracy z systemami telekomunikacyjnymi innych producentów,
    - G.722 – dla zapewnienia połączeń głosowych o podwyższonej jakości dźwięku,
    - kodek iLBC dla zapewnienia możliwości wykorzystywania terminali IP objętych systemem telekomunikacyjnym w lokalizacjach objętych łączami o słabych lub niegwarantowanych parametrach jakościowych QoS (np.

połączenia VPN) oraz kodek iSAC jako nowoczesny kodek adaptacyjny zapewniający wysoką jakość głosu,

- automatyczne wybieranie drogi (Auto Route Selection),
- możliwość routingu połączeń na bazie czasu i daty,
- narzędzia dynamicznego uaktualniania oprogramowania systemowego terminali,
- narzędzia dynamicznej wymiany routingu połączeń oraz informacji na temat planu numeracyjnego (Call Control Discovery) z innymi systemami komunikacyjnymi
- obsługę standardowych protokołów komunikacyjnych,
- H.323 - w zakresie komunikacji z bramami głosowymi oraz trunkami IP/H.323 do innych systemów telekomunikacyjnych,
- SIP - w zakresie: komunikacji z terminalami IP i bramami głosowymi oraz trunkami IP/SIP do innych systemów telekomunikacyjnych a także dla zapewniania przenoszenia informacji o dostępności użytkowników systemu,
- możliwość realizacji usługi wideotelefonii z wykorzystaniem terminali wideotelefonicznych,
- możliwość realizacji usługi wideotelefonii z wykorzystaniem aplikacji zainstalowanej na stacji roboczej,
- możliwość zabezpieczania sygnalizacji za pomocą standardowego protokołu TLS,
- możliwość zestawiania połączeń szyfrowanych w oparciu o standardowy protokół SRTP zarówno pomiędzy terminalami IP, jak też i do bram głosowych,
- system sterowania połączeniami telefonicznymi oraz wideo powinien pracować w trybie IPv4 oraz IPv6,
- system zarządzania połączeniami powinien współpracować z systemami rejestracji rozmów tel. w trybie aktywnym, tj. za pomocą konfiguracji przez administratora systemu zarządzania połączeniami dla telefonu abonenta, którego rozmowy mają być nagrywane drugiego strumienia VoIP (kierowanego do nagrywarki VoIP),
- system sterowania połączeniami powinien realizować funkcje kontroli wykorzystania pasma w sieci poprzez mechanizm Call Admission Control,
- mechanizmy Call Admission Control systemu sterowania połączeniami powinny współpracować z routerami IP w sieci LAN/WAN w celu rezerwacji pasma w sieci poprzez protokół RSVP dla połączeń telefonicznych w sieciach rozległych.

4. Terminale systemu muszą mieć możliwość dowolnego przenoszenia w obszarze sieci IP (np. przełączania do innych portów LAN) bez konieczności zmiany jakichkolwiek ustawień w systemie. Odłączenie i ponowne podłączenie terminala nie może powodować utraty bądź zmiany jego ustawień.
5. Współpraca z urządzeniami Gatekeeper H.323.
6. Dodawanie bram H.323, połączeń SIP trunk oraz współpraca z Gatekeeper H.323 powinno być elastyczne i nie powinno wymagać żadnych dodatkowych licencji w systemie.
7. System powinien mieć możliwość rejestrowania terminali wideo na bazie protokołu SIP w sposób umożliwiający zarządzanie nimi poprzez narzędzia administracyjne wbudowane w system.
8. System powinien mieć możliwość rejestrowania mostków audio oraz wideo w sposób umożliwiający zarządzanie nimi poprzez narzędzia administracyjne wbudowane w system.
9. System powinien realizować funkcjonalność poczty głosowej z możliwością tworzenia skrzynek poczty głosowej dla użytkowników.
10. System powinien umożliwiać rozbudowę do funkcjonalności tworzenia i obsługi indywidualnych zapowiedzi poczty głosowej przed przekierowaniem połączenia do skrzynki.

11. System powinien umożliwiać przyszłą rozbudowę do funkcjonalności tworzenia i obsługi indywidualnych zapowiedzi abonenckich przed zestawieniem połączenia przychodzącego do abonenta posiadającego pocztę głosową.
12. System powinien zapewniać dostęp dla każdego abonenta posiadającego pocztę głosową do aplikacji webowej, z której abonent może nagrać swoje powitanie oraz zmieniać ustawienia kierowania połączeń na pocztę głosową.
13. Dla każdego użytkownika poczty głosowej, po rozbudowie, system zapewnia możliwość integracji z pocztą elektroniczną w celu unifikacji wiadomości, co najmniej jako przesyłanie na konto emailowe abonenta informacji pozostawionych na poczcie głosowej w formie emaila z załącznikiem (funkcjonalność do potencjalnej rozbudowy systemu).
14. System musi realizować funkcje pojedynczego logowania (Single Sign-On, SSO) realizowane w oparciu o standard rynkowy Security Assertion Markup Language Single Sign-On (SAML SSO) dla użytkowników oraz administratorów systemu komunikacyjnego dla funkcji zarządzania połączeniami, informacji o dostępności oraz w celu konfiguracji funkcji poczty głosowej.
15. System musi realizować funkcje emitowania muzyki podczas zawieszenia obsługiwanego połączenia telefonicznego (ang. Music on Hold). Wymagana jest realizacja emitowania muzyki w sieci IP w trybie rozsiewczym (multicast) oraz w postaci indywidualnych, oddzielnych sesji (unicast).
16. System musi realizować funkcję cyfrowego serwera faksów w celu odbierania i nadawania faksów. Aplikacja serwera faksów musi zapewniać skrzynki faksowe dla pracowników oraz zapewniać jednoczesną transmisję wielu faksów jednocześnie.

Funkcje informacji o dostępności abonentów w systemie zunifikowanej komunikacji

System centralnego przetwarzania połączeń – zunifikowanej komunikacji po IP, powinien być uzupełnieniowy o system o dostępności abonentów, w zależności od rodzaju aparatów telefonicznych bądź aplikacji, wykorzystywanej w systemie powinien być realizowany z funkcjonalnościami, przedstawionymi poniżej (jeżeli aparat wspiera taką funkcjonalność):

1. System powinien umożliwiać agregację informacji o dostępności użytkownika korzystającego z różnych terminali i udostępniać ją na dla komunikatorów programowych oraz innych aplikacji wykorzystujących taką informację.
2. Możliwość pracy w klastrze w celu podniesienia niezawodności.
3. System powinien zapewniać przechowywanie indywidualnych list kontaktowych dla danego użytkownika.
4. System powinien wspierać protokoły standardowe SIP oraz XMPP.
5. System powinien wspierać funkcję „group chat” (czat z wieloma osobami jednocześnie).
6. System musi realizować funkcję zdalnego zarządzania połączeniami telefonicznymi realizowanymi z terminala abonenta poprzez funkcję CTI na bazie komunikatora abonenta. Funkcja sterowania telefonem musi być dostępna co najmniej dla abonentów wyposażonych w telefon IP, kompatybilny do sterowania poprzez CTI.
7. Informacja o dostępności powinna uwzględniać kilka źródeł informacji:

- zajętość abonenta w czasie rozmowy telefonicznej,
- w czasie połączenia wideo,
- zajętość wynikająca z zaplanowanego spotkania w kalendarzu,
- zajętość zdefiniowaną samodzielnie przez użytkownika poprzez wpis statusu obecności do komunikatora użytkownika.

8. System powinien zawierać aplikację komunikatora podstawowego dla użytkownika (na komputery PC z OS Windows oraz MacOS) o funkcjonalności obejmującej:

- informację o dostępności,
- obsługę komunikacji tekstowej (ang. IM, „chat”),
- sterowanie telefonem lub terminalem IP abonenta poprzez CTI.

9. System powinien zawierać aplikację komunikatora podstawowego na urządzenia mobilne dla użytkownika (co najmniej iPad, iPhone, Android) o funkcjonalności obejmującej:

- informację o dostępności,
- obsługę komunikacji tekstowej (ang. IM, „chat”).

10. System powinien zawierać aplikację komunikatora zaawansowanego dla użytkownika (na komputery PC z OS Windows oraz MacOS) o funkcjonalności obejmującej:

- informację o dostępności,
- komunikacji tekstowej (ang. IM, „chat”),
- sterowanie telefonem lub terminalem IP poprzez CTI,
- obsługę połączeń głosowych na bazie standardów G.711, G.722 oraz G.729a,
- obsługę połączeń wideo HD 720p na bazie standardu H.264/AVC,
- podgląd zawartości skrzynki poczty głosowej oraz odsłuchanie wiadomości ze skrzynki poczty głosowej.

11. System powinien mieć możliwość współpracy z aplikacją programowego komunikatora zaawansowanego na urządzenia mobilne (co najmniej iPad oraz iPhone) o funkcjonalności obejmującej:

- informację o dostępności,
- komunikacji tekstowej (ang. IM, „chat”),
- obsługę połączeń głosowych na bazie standardów G.711, G.722 oraz G.729a,
- obsługę połączeń wideo na bazie standardu H.264/AVC,
- podgląd zawartości skrzynki poczty głosowej oraz odsłuchanie wiadomości ze skrzynki poczty głosowej.

<u>Wymagania szczegółowe dla systemów/aplikacji uzupełniających system główny telefonii IP</u>

Wśród poszczególnych systemów, które powinny być dostarczone w ramach rozwiązania należy uwzględnić:

- System Contact Center – w podstawowej wersji, zapewniających podstawowe funkcjonalności, opisane w dalszej części,
- Zestaw/aplikacja sekretarska do wsparcia zarządzania i przełączania rozmów telefonicznych,
- System do obsługi faksów IP, zintegrowany na jednej platformie sprzętowej co system telefonii IP.

Należy podkreślić, że poszczególne systemy powinny być ze sobą w pełni zintegrowane, zainstalowane na pojedynczej platformie sprzętowej, jak system podstawowy/komunikacyjny, w zależności od wymagań w trybie wysokiej dostępności (klaster niezawodnościowy).

Funkcje centralnego Contact Center dla usług helpdesku w systemie zunifikowanej komunikacji

1. System komunikacyjny powinien realizować funkcje zapowiedzi słownych IVR oraz dystrybucji wywołań ACD dla grupy agentów w ramach centralnego Contact Center, przeznaczonego dla usług helpdesku.

2. System musi umożliwiać terminowanie połączeń telefonicznych i ich automatyczną obsługę przez system zapowiedzi IVR (Interactive Voice Responder), definiowaną przez skrypty budowane przez graficzne narzędzie. Obsługa skryptu musi umożliwiać:

- odgrywanie zapowiedzi głosowych (pliki .wav),
- odczyt i interpretację sygnałów DTMF,
- możliwość sięgania do danych w źródłach HTTP/XML,
- odczytywanie danych systemowych takich jak liczba osób oczekujących w kolejkach, średni czas oczekiwania itp.,
- możliwość przesyłania danych do programu, którym dysponuje agent systemu na swoim komputerze PC,
- kolejkowanie połączenia do wybranej kolejki z przypisaną do nich grupą agentów,
- zarezerwowanie zdefiniowanego czasu dla zamknięcia połączenia, do celów sporządzenia notatki oraz wpisania danych do innych aplikacji.

3. System powinien mieć możliwość rozbudowy o funkcjonalność umożliwiającą w ramach funkcji skryptu IVR pobieranie i zapis informacji do zewnętrznych baz danych (SQL).
4. System powinien obsługiwać co najmniej 5 agentów Contact Center jednocześnie oraz co najmniej 100 jednoczesnych kanałów IVR.
5. W ramach kolejkowania połączeń system powinien mieć możliwość obsługi wielu kanałów komunikacji, co najmniej: telefonię (głos) i połączenia wideo.
6. System musi realizować funkcje kolejkowania Contact Center dla połączeń głosowych oraz dla połączeń wideo.
7. System powinien mieć możliwość rozbudowy o dodatkowe kanały i kolejkę dla komunikacji, co najmniej: email oraz web czat dla każdego z Agentów.
8. Agenci Contact Center będący abonentami systemu są delegowani do obsługi kolejek ACD i muszą posiadać aplikację webową na PC dedykowaną do obsługi połączeń oraz edycji stanu gotowości (gotowy/nie gotowy/wylogowany) do przyjmowania kolejnych połączeń.
9. Agenci Contact Center muszą mieć możliwość wykorzystania telefonu IP z aplikacją XML zamiast aplikacji webowej na PC) do obsługi połączeń oraz edycji stanu gotowości (gotowy/nie gotowy/wylogowany) do przyjmowania kolejnych połączeń.
10. System powinien realizować funkcje nadzorcze w zakresie podglądu stanu kolejek ACD w Contact Center oraz poszczególnych agentów.
11. System powinien realizować funkcje nadzorcze w zakresie generowania raportów historycznych oraz bieżących z pracy systemu oraz pracy poszczególnych agentów.
12. Funkcje Contact Center powinny być realizowane przez aplikację opartą o protokół IP oraz zintegrowany z systemem sterowania oraz bramami głosowymi systemu telefonii. Nie dopuszcza stosowania systemów hybrydowych, gdzie serwer ACD jest wyposażony w oddzielne interfejsy TDM.
13. Funkcje Contact Center powinny uwzględniać kierowanie połączeń na bazie umiejętności (skills based routing), co najmniej 50 zdefiniowanych kategorii umiejętności oraz 10 poziomów umiejętności Agenta.
14. System powinien mieć możliwość obsługi funkcji nadzorczej (Supervisor) w Contact Center w formie dedykowanej aplikacji na PC, do zarządzania pracą i monitorowania kolejek Contact Center.
15. System powinien mieć możliwość rozbudowy funkcji Contact Center dla helpdesku o kolejnych agentów dla co najmniej 100 aktywnych agentów łącznie bez konieczności wymiany platformy sprzętowej.

16. System powinien mieć możliwość rozbudowy do klastra niezawodnościowego (HA) z możliwością pracy w trybie rozproszonym, w którym serwery klastra Contact Center połączone są poprzez sieć IP, co najmniej LAN oraz WAN.

Zestaw do wsparcia/zarządzania rozmowami telefonicznymi – aplikacja sekretarska powinien umożliwiać:

1. Konsola telefoniczna dla recepcji musi być dedykowanym oprogramowaniem realizującym funkcje zarządzania połączeniami dla funkcji recepcji, zintegrowanym z systemem komunikacyjnym.
2. Musi realizować funkcje obsługi połączeń dla recepcji w zakresie: odbierania połączeń, przekierowania, zawieszania, parkowania, obsługi konferencji oraz zestawiania nowych połączeń.
3. Musi być aplikacją graficzną i prezentować na ekranie poszczególne panele informacyjne:

- panel sterowania połączeniami zawierający kontrolki wymagane do funkcji obsługi połączeń,
- lista kontaktów,
- lista połączeń zaparkowanych,
- podgląd historii połączeń.

4. Musi mieć możliwość dopasowania wyglądu do preferencji obsługi recepcji w zakresie co najmniej:

- rozmieszczenia oraz rozmiaru paneli informacyjnych,
- zmiany wielkości czcionki w aplikacji konsoli.

5. Musi mieć możliwość tworzenia listy kontaktów, wyszukiwania z listy kontaktów, grupowania kontaktów.
6. Lista kontaktów konsoli powinna być tworzona na kilka sposobów: poprzez pobranie jej z systemu komunikacyjnego, poprzez import pliku tekstowego CSV oraz poprzez samodzielne, manualne dodanie kontaktów.
7. W zakresie obsługi połączeń konsola musi współpracować oraz sterować terminalem stanowiącym wyposażenie recepcji. Jako terminal stanowiący wyposażenie recepcji rozumie się telefon IP albo komunikator zaawansowany na PC z systemem Windows wraz z przypisanymi liniami telefonicznymi.
8. W zakresie obsługi połączeń konsola musi obsługiwać połączenia głosowe oraz wideo, zależnie od typu terminala stanowiącego wyposażenie recepcji.
9. Konsola musi wyświetlać statusy obecności dla abonentów systemu komunikacyjnego, którzy znajdują się na liście kontaktów konsoli.
10. Musi pracować na samodzielnym komputerze PC oraz wspierać systemy operacyjne co najmniej Windows 7, Windows 8 oraz Windows 8.1. Nie dopuszcza się rozwiązania, w którym do obsługi konsoli potrzebny jest dodatkowy serwer zarządzający funkcjami konsoli.
11. Musi wspierać obsługę w jęz. polskim lub angielskim.
12. Musi posiadać mechanizmy administracyjne zabezpieczające przed przypadkową zmianą ustawień konfiguracji konsoli przez jej użytkownika.

System do realizacji funkcjonalności faksowych w oparciu o platformę IP, funkcjonalnościami:

1. Wysyłania i odbierania faksów, poprzez łącze cyfrowe, terminowane na bramie głosowej całego systemu telefonii IP,
2. Wydruku dokumentów odebranych poprzez faks,
3. Możliwością podłączenia zeskanowanych dokumentów do wysłania faksem,
4. Integrację z systemem telefonii, w tym komunikatorem instalowanym na końcówkach (komputery),
5. Integracja z pocztą elektroniczną.
6. Obsługa 8 kanałów komunikacyjnych jednocześnie, z możliwością ich rozszerzenia w ramach licencji.

Wymagania szczegółowe dla poszczególnych telefonów – końcówek systemu telefonii IP

Telefony powinny być dostarczone w wersjach, umożliwiających ich wykorzystanie w zależności od potrzeb poszczególnych użytkowników systemu telefonicznego, w ilościach przewidzianych powyżej. Poniżej przedstawione są wymagania ogólne dla poszczególnych aparatów telefonicznych, przy czym zakłada się, że powinny pochodzić od tego samego producenta, co cały system telefonii IP, w celu realizacji odpowiedniego poziomu integracji i możliwości wykorzystania systemu, w zależności od wymaganych potrzeb.

Telefon uproszczony – EC1 (pozycja nr 9 w tabeli powyżej)

1. Urządzenie musi wspierać kodeki audio co najmniej określone przez standardy G.711u, G.729a.
2. Urządzenie musi posiadać wyświetlacz graficzny o rozdzielczości co najmniej 128 x 32 piksele, umożliwiający wyświetlanie w dwóch liniach informacji na temat aktualnego czasu (data i godzina), ustawień urządzenia oraz stanu połączenia.
3. Urządzenie musi posiadać możliwość konfiguracji co najmniej 1 linii (numeru telefonicznego).
4. Urządzenie musi na bieżąco w czasie trwania rozmowy umożliwiać wyświetlanie poprzez przeglądarkę internetową informacji diagnostycznych o połączeniu (rodzaj kodeka, liczba wysłanych, odebranych i zgubionych pakietów z próbkami głosowymi, zmienność opóźnienia przesyłania tych pakietów – używane dla celów diagnostycznych w przypadku konieczności diagnozowania przez administratorów problemów z jakością transmisji głosu w systemie telekomunikacyjnym.
5. Urządzenie musi posiadać wbudowany system głośnomówiący (tzw. speakerphone), umożliwiający prowadzenie rozmowy bez podnoszenia słuchawki i działający w trybie full-dupleks.
6. Urządzenie musi mieć możliwość montażu na ścianie.
7. Urządzenie musi posiadać poniższe dedykowane przyciski funkcyjne:

- przycisk dostępu do ustawień urządzenia,
- przycisk ponownego wybierania,
- przycisk przekierowania rozmowy,
- przycisk zawieszenia połączenia,
- przycisk sterujący głośnością,
- przycisk wyłączenia mikrofonu,
- przycisk trybu rozmowy przez system głośnomówiący,

8. Urządzenie musi posiadać dwukierunkowy (góra/dół) przycisk nawigacyjny umożliwiający poruszanie się po różnych menu.
9. Urządzenie musi posiadać wbudowany przełącznik Ethernet, z dwoma portami 10/100 Mb/s, jeden w kierunku przełącznika sieciowego, drugi dedykowany do dołączenia PC.
10. Port przełącznika urządzenia w kierunku przełącznika sieciowego powinien wspierać trunking 802.1Q celem odseparowania ruchu głosu i ruchu danych.
11. Transmisja głosu oraz danych z komputera PC dołączonego do urządzenia muszą być przesyłane w dwóch różnych sieciach VLAN.
12. Urządzenie musi umożliwiać zasilanie go z sieci komputerowej LAN zgodnie ze standardem PoE IEEE oraz z wykorzystaniem lokalnych zasilaczy (transformujących napięcie z sieci 230V).
13. Urządzenie musi być energooszczędne i pracować w klasie 1 PoE zgodnie z IEEE 802.3af.
14. Menu urządzenia musi być zrealizowane w języku polskim oraz angielskim, przy czym wymagane jest, aby możliwa była zmiana rodzaju języka menu w zależności od ustawień w profilu zalogowanego na nim użytkownika.
15. Urządzenie musi wspierać funkcjonalność wykrywania ciszy (Voice Activity Detection) i niewysyłaniu pakietów głosowych IP w czasie jej trwania.
16. Urządzenie musi wspierać funkcjonalność generowania szumu (Comfort Noise Generation) podczas rozmowy w czasie trwania ciszy.
17. Urządzenie musi posiadać lampkę sygnalizującą oczekującą wiadomość poczty głosowej (MWI).
18. Urządzenie musi zapewniać wsparcie dla protokołu sterującego SIP.
19. Urządzenie musi zapewniać wsparcie dla protokołów sieciowych TFTP, DHCP, DNS.
20. Urządzenie musi obsługiwać pobieranie oraz wymianę plików konfiguracyjnych oraz oprogramowania z systemu zarządzania połączeniami.

Telefon podstawowy – EC2 (pozycja nr 10 w tabeli powyżej)

1. Urządzenie obsługuje kodeki audio co najmniej określone przez standardy G.711a, G.711u, G.729ab, G.722 oraz iLBC.
2. Urządzenie posiada monochromatyczny, podświetlany wyświetlacz (minimum 396 x 162 piksele), umożliwiający obsługę urządzenia, odczytywanie informacji i wywoływanie funkcji urządzenia. Wymagana przekątna wyświetlacza co najmniej 3,5 cala.
3. Urządzenie posiada co najmniej 2 przyciski z podświetleniem LED w trybie tri-color wbudowanym w przycisk, umożliwiające wybór linii oraz obserwację jej stanu (zajętość/dostępność), bądź też obserwację stanu linii innego urządzenia w systemie.
4. Urządzenie ma możliwość skonfigurowania co najmniej 2 różnych linii (numerów) telefonicznych.
5. Urządzenie posiada co najmniej 4 przycisków umożliwiających obsługę funkcji menu prezentowanych na wyświetlaczu.
6. Urządzenie w czasie trwania rozmowy umożliwia wyświetlanie na bieżąco lokalnie na jego ekranie, a także zdalnie poprzez przeglądarkę internetową, informacji diagnostycznych o połączeniu (rodzaj kodeka, liczba wysłanych, odebranych i zgubionych pakietów z próbkami głosowymi, zmienność opóźnienia przesyłania tych pakietów), używane dla celów diagnostycznych w przypadku konieczności

diagnozowania przez administratorów problemów z jakością transmisji głosu w systemie telekomunikacyjnym.

7. Urządzenie posiada wbudowany system głośnomówiący (tzw. speakerphone), umożliwiający prowadzenie rozmowy bez podnoszenia słuchawki i działający w trybie full-dupleks.
8. Wbudowany głośnik, a także słuchawka i mikrofon urządzenia są gotowe sprzętowo do transmisji głosu w trybie szerokopasmowym (G.722).
9. Urządzenie posiada dedykowane gniazdo do podłączenia zestawu nagłownego. Nie jest dopuszczalne rozwiązanie gdzie zestaw nagłowny dołącza się zamiast albo razem ze słuchawką na tym samym gnieździe.
10. Urządzenie obsługuje funkcję zestawiania i obsługi połączeń poprzez EHS (ang. Electronic Hook Switch) oraz posiada dedykowane gniazdo do podłączenia zestawu nagłownego z obsługą funkcji EHS.
11. Urządzenie posiada poniższe dedykowane przyciski funkcyjne:

- przycisk dostępu do listy kontaktów,
- przycisk dostępu do ustawień urządzenia,
- przycisk dostępu do funkcji transferu rozmów,
- przycisk dostępu do konferencji,
- przycisk dostępu do zawieszania połączeń,
- przycisk dostępu do poczty głosowej,
- przycisk sterujący głośnością,
- przycisk Mute (wyłączenie mikrofonu),
- przycisk trybu Headset (rozmowa przez system nagłowny),
- przycisk trybu Speaker (rozmowa przez system głośnomówiący).

12. Urządzenie posiada dwukierunkowy (góra/dół) przycisk nawigacyjny umożliwiający poruszanie się po różnych menu.
13. Urządzenie posiada wbudowany przełącznik Ethernet, z dwoma portami 10/100 Mbps, jeden w kierunku przełącznika sieciowego, drugi dedykowany do dołączenia PC.
14. Port przełącznika urządzenia w kierunku przełącznika sieciowego wspiera trunking 802.1Q celem odseparowania ruchu głosu i ruchu danych.
15. Transmisja głosu oraz danych z komputera PC dołączonego do urządzenia są przesyłane w dwóch różnych sieciach VLAN.
16. Urządzenie umożliwia zasilanie go z sieci komputerowej LAN zgodnie ze standardem PoE IEEE oraz z wykorzystaniem lokalnych zasilaczy (transformujących napięcie z sieci 230V).
17. Urządzenie jest energooszczędne i pracuje w klasie 1 IEEE 802.3af (do 3,84W).
18. Urządzenie realizuje przy współpracy z systemem centralnym zdefiniowany harmonogram zasilania poprzez funkcje uśpienia (np. po godzinach pracy biura) oraz wybudzenia urządzenia.
19. Menu urządzenia jest zrealizowane w języku polskim oraz angielskim, przy czym możliwa jest zmiana rodzaju języka menu w zależności od ustawień w profilu zalogowanego na nim użytkownika.
20. Urządzenie jest wyposażone w podstawkę umożliwiającą ustawienie urządzenia na płaskiej powierzchni w co najmniej dwóch pozycjach.

21. Musi ma możliwość dostosowania do montażu na ścianie.
22. Urządzenie zapewnia wsparcie dla protokołu sterującego SIP.
23. W zakresie bezpieczeństwa urządzenie pozwala na:

- zabezpieczenie komunikacji z serwerem sterującym za pomocą TLS,
- zabezpieczenie strumienia audio za pomocą SRTP,
- wsparcie autentykacji 802.1X,
- obsługę certyfikatów cyfrowych,
- obsługę szyfrowanych plików konfiguracyjnych,
- autentykację oprogramowania urządzenia.

24. Urządzenie obsługuje aplikacje w języku XML, w tym aplikacje XML innych producentów.
25. Urządzenie obsługuje pobieranie oraz wymianę plików konfiguracyjnych oraz oprogramowania (firmware) z systemu zarządzania połączeniami.
26. Urządzenie obsługuje oprogramowanie (firmware) podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez system zarządzania połączeniami.
27. Urządzenie obsługuje protokół LLDP, CDP lub równoważny w celu poprawnej współpracy z przełącznikami LAN w zakresie negocjacji parametrów połączenia oraz dostarczonego zasilania POE.
28. Urządzenie powinno być zarządzane centralnie poprzez system komunikacyjny Zamawiającego w zakresie co najmniej:

- pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych Zamawiającego,
- obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne Zamawiającego,
- możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki konferencyjne),
- możliwości zdalnego restartu urządzenia lub grupy urządzeń,
- możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego,
- zmiany numeru linii abonenta oraz edycji opisu linii abonenta,
- konfiguracji ustawień i opisów klawiszy aparatu,
- konfiguracji uprawnień oraz klasy usług abonenckich,
- wykonania zdalnego restartu urządzenia z wymuszeniem pobrania nowej konfiguracji,
- wykonania zdalnego resetu urządzenia z wymuszeniem pobrania nowego oprogramowania (firmware) oraz nowej konfiguracji,
- wykonania zdalnego restartu oraz resetu dla grupy urządzeń, wyspecyfikowanej przez administratora z puli wszystkich urządzeń,
- uruchomienia w urządzeniu funkcji bezpieczeństwa (TLS oraz sRTP),
- włączenia funkcjonalności w zakresie 802.1X,
- uruchomienia w urządzeniu serwisu logowania abonenta na telefonie,
- dodania do urządzenia serwisów XML.

Terminal wideo IP – EC3 (pozycja nr 11 w tabeli)

1. Urządzenie musi pełnić funkcję personalnego terminala wideo przeznaczonego do pracy na biurku.

2. Musi posiadać zintegrowany w jednej obudowie dotykowy monitor LCD, mikrofony, nagłośnienie, kamerę, podstawę do ustawienia terminala na biurku oraz kodek wideokonferencyjny.
3. Monitor musi posiadać rozdzielczość co najmniej 1920 x 1080 pikseli.
4. Urządzenie musi wspierać kodek audio szerokopasmowy zgodnie ze specyfikacją ISO AAC-LD (Advanced Audio Coding - Low Delay) oraz ze standardem G.722, przy czym mikrofony oraz głośnik urządzenia powinny umożliwiać wykorzystanie możliwości tego kodeka tak by zapewnić wysoką jakość rozmowy telefonicznej.
5. Urządzenie musi wspierać kodeki audio co najmniej określone przez standardy G711a, G711μ i G729a, G729ab tak by umożliwić współpracę z telefonami IP starszych generacji, nie obsługującymi kodeków szerokopasmowych, a także rozwiązaniami systemów telekomunikacyjnych innych producentów.
6. Urządzenie musi wspierać kodek audio wąskopasmowy działający zgodnie ze standardami Internet Speech Audio Codec (iSAC) oraz Internet Low Bitrate Codec (iLBC) – dla zapewnienia możliwości wykorzystywania telefonów w placówkach objętych łączami o słabych lub niegwarantowanych parametrach jakościowych QoS.
7. Urządzenie musi realizować połączenia wideo na bazie standardu H.264 Advanced Video Coding (AVC) i umożliwiać kodowanie oraz dekodowanie obrazu wideo z prędkością nie mniejszą niż 30 ramek na sekundę dla rozdzielczości co najmniej:

- CIF (352 x 288 pikseli),
- VGA (640 x 480 pikseli),
- SVGA (800 x 600 pikseli),
- XGA (1024 x 768 pikseli),
- w448p (768 x 448 pikseli),
- w576p (1024 x 576 pikseli),
- 720p (1280 x 720 pikseli),
- 1080p (1920 x 1080 pikseli).

8. Urządzenie musi umożliwiać jednoczesne przesyłanie i odbieranie równolegle do strumienia wideo drugiego strumienia prezentacyjnego, na bazie standardowego protokołu SIP Binary Floor Control Protocol (BFCP) w rozdzielczości 1080p (1920 x 1080 pikseli).
9. Urządzenie musi posiadać wbudowany dotykowy monitor LCD, umożliwiający jego wygodną obsługę, odczytywanie informacji i wywoływanie funkcji urządzenia oraz musi obsługiwać wyświetlanie na nim ruchomego strumienia wideo. Monitor musi posiadać minimalne parametry:

- rozdzielczość 1920 x 1080, 1080p w układzie 16:9,
- przekątna min. 23 cale,
- kontrast 1000:1,
- kąt widzenia 178 stopni,
- zmiana kąta położenia monitora,
- czas reakcji 5 ms,
- jasność 215 cd/mkw,
- paleta kolorów 24-bitowa (16.7 milionów kolorów),
- obsługa funkcji multi-touch dla 10-punktowego multi-touch,
- musi pokazywać podgląd z kamery (self-view),
- musi wyświetlać obraz z dołączonego PC rozdzielczość co najmniej 1080p,
- musi wyświetlać obraz strony zdalnej z połączenia wideo rozdzielczość co najmniej 1080p.

10. Urządzenie musi posiadać wbudowaną kamerę wideo o parametrach co najmniej:

- rozdzielczość i tryb pracy co najmniej 1080p30,

- kąt widzenia 63 stopnie,
- tryb pracy kamery dokumentowej z automatycznym odwróceniem obrazu,
- manualna regulacja kąta kamery względem prostopadłej do ekranu w zakresie od -5 stopni do 70 stopni,
- mechaniczna zasłona obiektywu kamery dla zachowania prywatności.

11. Urządzenie musi posiadać płynną regulację umożliwiającą ustawienie ekranu w co najmniej 3 pozycjach, w zakresie od 11 stopni do 50 stopni względem pionu, dopasowując kąt wyświetlacza do preferencji użytkownika.

12. W zakresie bezpieczeństwa urządzenie musi pozwalać na:

- zabezpieczenie komunikacji z serwerem sterującym za pomocą TLS,
- zabezpieczenie strumienia audio oraz wideo za pomocą SRTP,
- obsługa protokołu HTTPS,
- obsługa protokołów EAP-FAST, EAP-TLS dla LAN,
- obsługa WPA2 (EAP-FAST) dla komunikacji WLAN,
- obsługa EAP-TLS dla komunikacji WLAN,
- obsługa PEAP-GTC dla komunikacji WLAN,
- obsługa certyfikatów cyfrowych fabrycznych oraz certyfikatów cyfrowych lokalnych,
- obsługa protokołu X.509 Digital Certificates (DER encoded binary), DER oraz Base-64. Obsługa certyfikatów z kluczami 1024, 2048, 4096,
- możliwość administracyjnego wyłączenia interfejsów WLAN oraz Bluetooth urządzenia,
- blokowanie urządzenia z wymuszeniem podania PIN lub hasła dostępowego,
- możliwość całkowitego usunięcia wszystkich danych z urządzenia w kilku trybach: samodzielnie przez użytkownika, zdalnie przez administratora oraz automatycznie po nieudanych próbach zalogowania,
- musi posiadać Kensington Security Slot,
- obsługa autentykacji PC dołączonego do urządzenia na bazie mechanizmów IEEE 802.1X.

13. Urządzenie musi posiadać dedykowane gniazda, co najmniej:

- 3 porty USB do dołączenia urządzeń peryferyjnych (klawiatura, mysz, słuchawki) zapewniające zasilanie 500 mA przy 5V (moc 2.5W),
- 1 port wejściowy HDMI do dołączenia komputera PC,
- 1 gniazdo na kartę Micro Secure Digital (SD).

14. Urządzenie musi posiadać co najmniej następujące dedykowane przyciski:

- przycisk wyciszenia (mute),
- przycisk zmiany głośności.

15. Urządzenie musi dawać dostęp do systemowej książki telefonicznej, historii połączeń oraz zaplanowanych spotkań wideokonferencyjnych w kalendarzu

16. Urządzenie musi obsługiwać co najmniej 1 linię (numer telefoniczny)

17. Urządzenie musi współpracować z systemem zarządzania połączeniami w celu realizacji funkcji co najmniej:

- definiowania numeru E.164 oraz adresu URI przypisanego do terminala, zapewniając obsługę zarówno połączeń wideo wraz z kanałem prezentacyjnym, jak i połączeń głosowych,
- definiowania uprawnień oraz ograniczeń abonenckich poprzez możliwość blokowania połączeń na numery wysokopłatne oraz międzynarodowe,
- definiowania uprawnień w zakresie dopuszczenia połączeń wideo poprzez sieć WAN za pomocą mechanizmów Call Admission Control,
- możliwości tworzenia linii współdzielonych z terminalami telefonicznymi w systemie przetwarzania połączeń, w tym także z telefonami GSM zdefiniowanymi w systemie w profilach użytkowników,

- funkcje abonenckie takie jak: dostęp do skrzynki poczty głosowej, przekierowanie (call forward), przekazanie połączenia (call transfer),
- funkcja nie przeszkadzać (do not disturb DND),
- zawieszenie połączenia (Hold),
- centralna oraz prywatna książka telefoniczna.

18. Urządzenie musi posiadać wbudowany przełącznik Ethernet, z dwoma portami 10/100/1000 Mbps
19. Port przełącznika urządzenia w kierunku przełącznika sieciowego powinien wspierać trunking 802.1Q celem odseparowania ruchu głosu i ruchu danych.
20. Transmisja głosu/obrazu oraz danych z komputera PC dołączonego do urządzenia muszą być przesyłane w dwóch różnych sieciach VLAN.
21. Urządzenie musi zapewniać wsparcie dla standardowego protokołu sterującego SIP oraz H.323.
22. Urządzenie musi posiadać wbudowany interfejs bezprzewodowy WLAN zgodny ze standardami 802.11 a/b/g/n, umożliwiający użytkowanie go w miejscach, gdzie z powodów technologicznych lub estetycznych byłoby niemożliwe lub niewskazane dołączanie do sieci LAN.
23. Urządzenie musi posiadać wbudowany interfejs bezprzewodowy Bluetooth 3.0 z Enhanced Data Rate (EDR) do obsługi urządzeń peryferyjnych.
24. Urządzenie musi obsługiwać bezprzewodowe współdzielenie prezentacji z PC.
25. Urządzenie musi mieć możliwość zalogowania się na nim użytkownika z przypisanym profilem. Wraz z zalogowaniem do urządzenia zostają do niego przypisane parametry profilu zalogowanego abonenta takie, jak: numer linii, uprawnienia abonenckie, ustawienia obsługi połączeń, które zdefiniowane są centralnie w systemie zarządzania połączeniami.
26. Urządzenie musi obsługiwać funkcję uproszczonego dołączenia do zaplanowanego spotkania wideokonferencyjnego, realizowanego przez pojedyncze naciśnięcie przycisku na ekranie dotykowym.
27. Menu urządzenia powinno być zrealizowane w języku polskim oraz angielskim, przy czym wymagane jest, aby możliwa była zmiana rodzaju języka menu w zależności od ustawień w profilu zalogowanego na nim użytkownika.
28. Urządzenie musi być dostarczone wraz z zasilaczem AC 230V.
29. Urządzenie musi być przystosowane do montażu VESA, do zastosowania np. przy montażu urządzenia do ściany lub do konstrukcji mobilnych
30. Wraz z urządzeniem muszą być zapewnione przewody:

- patchcord o długości co najmniej 2.5 metra, umożliwiający dołączenie go do gniazda sieci LAN,
- przewód HDMI do dołączenia PC o długości co najmniej 2 metry.

31. Urządzenie musi posiadać otwarty interfejs programistyczny API do sterowania połączeniami i do konfiguracji ustawień urządzenia. Musi posiadać możliwość integracji i sterowania poprzez API oraz skrypty programistyczne elementów infrastruktury pomieszczenia (HVAC), takich jak oświetlenie, wybór wejścia i wyjścia w matrycy wideo, zasłanianie rolet.
32. Urządzenie powinno być zarządzane centralnie poprzez system komunikacyjny Zamawiającego w zakresie co najmniej:

- pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych Zamawiającego,

- obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne Zamawiającego,
- możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU),
- możliwości zdalnego restartu urządzenia lub grupy urządzeń,
- możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego.

33. Wszystkie elementy rozwiązania muszą pochodzić od jednego producenta i być objęte wspólną gwarancją i serwisem producenta.

Telefon rozszerzony, monochromatyczny z klawiszami szybkiego wybierania – EC4 (pozycja nr 12 z tabeli)

1. Urządzenie musi wspierać kodeki audio co najmniej określone przez standardy G.711a, G.711u, G.729ab, G.722 oraz iLBC.
2. Urządzenie musi posiadać monochromatyczny, podświetlany wyświetlacz (minimum 396 x 162 piksele), umożliwiający obsługę urządzenia, odczytywanie informacji i wywoływanie funkcji urządzenia. Wymagana przekątna wyświetlacza co najmniej 3,5 cala.
3. Urządzenie musi posiadać co najmniej 16 przycisków z podświetleniem LED w trybie tri-color wbudowanym w przycisk, umożliwiające wybór linii oraz obserwację jej stanu (zajętość/dostępność), bądź też obserwację stanu linii innego urządzenia w systemie.
4. Urządzenie musi mieć możliwość skonfigurowania co najmniej 16 różnych linii (numerów) telefonicznych.
5. Urządzenie musi posiadać co najmniej 4 przyciski umożliwiające obsługę funkcji menu prezentowanych na wyświetlaczu.
6. Urządzenie musi mieć kolor ciemny.
7. Urządzenie musi na bieżąco w czasie trwania rozmowy umożliwiać wyświetlanie lokalnie na jego ekranie, a także zdalnie poprzez przeglądarkę internetową, informacji diagnostycznych o połączeniu (rodzaj kodeka, liczba wysłanych, odebranych i zgubionych pakietów z próbkami głosowymi, zmienność opóźnienia przesyłania tych pakietów), używane dla celów diagnostycznych w przypadku konieczności diagnozowania przez administratorów problemów z jakością transmisji głosu w systemie telekomunikacyjnym.
8. Urządzenie musi posiadać wbudowany system głośnomówiący (tzw. speakerphone), umożliwiający prowadzenie rozmowy bez podnoszenia słuchawki i działający w trybie full-dupleks.
9. Wbudowany głośnik, a także słuchawka i mikrofon urządzenia muszą być gotowe sprzętowo do transmisji głosu w trybie szerokopasmowym (G.722).
10. Urządzenie musi posiadać dedykowane gniazdo do podłączenia zestawu nagłownego. Nie jest dopuszczalne rozwiązanie, gdzie zestaw nagłowny dołącza się zamiast albo razem ze słuchawką na tym samym gnieździe.
11. Urządzenie musi obsługiwać funkcję zestawiania i obsługi połączeń poprzez EHS (ang. Electronic Hook Switch) oraz musi posiadać dedykowane gniazdo do podłączenia zestawu nagłownego z obsługą funkcji EHS.
12. Urządzenie musi posiadać poniższe dedykowane przyciski funkcyjne:

- przycisk dostępu do listy kontaktów,
- przycisk dostępu do ustawień urządzenia,
- przycisk dostępu do funkcji transferu rozmów,
- przycisk dostępu do konferencji,
- przycisk dostępu do zawieszania połączeń,
- przycisk dostępu do poczty głosowej,
- przycisk sterujący głośnością,
- przycisk Mute (wyłączenie mikrofonu),
- przycisk trybu Headset (rozmowa przez system nagłowny),
- przycisk trybu Speaker (rozmowa przez system głośnomówiący).

13. Urządzenie musi posiadać dwukierunkowy (góra/dół) przycisk nawigacyjny umożliwiający poruszanie się po różnych menu.
14. Urządzenie musi posiadać wbudowany przełącznik Ethernet, z dwoma portami 10/100 Mbps, jeden w kierunku przełącznika sieciowego, drugi dedykowany do dołączenia PC.
15. Port przełącznika urządzenia w kierunku przełącznika sieciowego powinien wspierać trunking 802.1Q celem odseparowania ruchu głosu i ruchu danych.
16. Transmisja głosu oraz danych z komputera PC dołączonego do urządzenia muszą być przesyłane w dwóch różnych sieciach VLAN.
17. Urządzenie musi umożliwiać zasilanie go z sieci komputerowej LAN zgodnie ze standardem PoE IEEE oraz z wykorzystaniem lokalnych zasilaczy (transformujących napięcie z sieci 230V).
18. Urządzenie musi być energooszczędne i pracować w klasie 1 IEEE 802.3af.
19. Menu urządzenia musi być zrealizowane w języku polskim oraz angielskim, przy czym wymagane jest, aby możliwa była zmiana rodzaju języka menu w zależności od ustawień w profilu zalogowanego na nim użytkownika.
20. Urządzenie musi być wyposażone w podstawkę umożliwiającą ustawienie urządzenia na płaskiej powierzchni w co najmniej dwóch pozycjach.
21. Musi mieć możliwość dostosowania do montażu na ścianie.
22. Urządzenie musi zapewniać wsparcie dla protokołu sterującego SIP.
23. W zakresie bezpieczeństwa urządzenie musi pozwalać na:

- zabezpieczenie komunikacji z sewerem sterującym za pomocą TLS,
- zabezpieczenie strumienia audio za pomocą SRTP,
- wsparcie autentykacji 802.1X,
- obsługę certyfikatów cyfrowych,
- obsługę szyfrowanych plików konfiguracyjnych,
- autentykację oprogramowania urządzenia,.

24. Urządzenie musi obsługiwać aplikacje w języku XML, w tym aplikacje XML innych producentów.
25. Urządzenie powinno być zarządzane centralnie poprzez system komunikacyjny Zamawiającego w zakresie co najmniej:

- pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych Zamawiającego,
- obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne Zamawiającego,
- możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU),

- możliwości zdalnego restartu urządzenia oraz wybranej grupy urządzeń,
- możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego.

Telefon zaawansowany z kolorowym wyświetlaczem z modułem klawiszy programowalnych, szybkiego wybierania – EC5 (pozycja nr 13 z tabeli)

Urządzenie musi wspierać kodek audio szerokopasmowy zgodnie ze standardem G.722, przy czym słuchawka, mikrofon oraz głośnik aparatu powinny umożliwiać wykorzystanie możliwości tego kodeka tak by zapewnić wysoką jakość rozmowy telefonicznej.

1. Urządzenie powinno być dostarczone w kolorze białym.
2. Urządzenie musi wspierać kodeki audio co najmniej określone przez standardy G.711a, G.711μ i G.729a tak by umożliwić współpracę z telefonami IP starszych generacji, nie obsługującymi kodeków szerokopasmowych, a także rozwiązaniami systemów telekomunikacyjnych innych producentów.
3. Urządzenie musi wspierać kodeki audio działające zgodnie ze standardem iLBC (Internet Low Bitrate Codec) oraz iSAC (internet Speech Audio Codec) – dla zapewnienia możliwości wykorzystania telefonów w placówkach objętych łączami o słabych lub niegwarantowanych parametrach jakościowych QoS.
4. Urządzenie musi posiadać duży, o przekątnej min. 5 cali, kolorowy ekran wysokiej jakości (minimum 800x480 pikseli), umożliwiający jego wygodną obsługę, odczytywanie informacji i wywoływanie funkcji urządzenia.
5. Urządzenie musi posiadać regulację umożliwiającą ustawienie ekranu w co najmniej dwóch pozycjach, dopasowując kąt wyświetlacza do preferencji użytkownika. Urządzenie musi mieć kolor ciemny.
6. Urządzenie musi zawierać co najmniej 5 przycisków z podświetleniem wbudowanym w przycisk, umożliwiających wybór linii oraz obserwację jej stanu (zajętość/dostępność), bądź też obserwację stanu linii innego urządzenia w systemie. Urządzenie musi umożliwiać zwiększenie liczby takich przycisków przez dołączenie do niego dodatkowych przystawek.
7. Urządzenie musi mieć możliwość doposażania w dodatkowe przystawki zwiększające ilość takich fizycznych przycisków o co najmniej 36 przycisków.
8. W zakresie bezpieczeństwa urządzenie musi pozwalać na:

- zabezpieczenie komunikacji z serwerem sterującym za pomocą TLS,
- zabezpieczenie strumienia audio za pomocą sRTP.

9. Urządzenie musi mieć wbudowane oprogramowanie klienta VPN w celu szyfrowania transmisji.
10. Urządzenie musi na bieżąco w czasie trwania rozmowy umożliwiać wyświetlanie lokalnie na jego ekranie, a także zdalnie poprzez przeglądarkę internetową, informacji diagnostycznych o połączeniu (rodzaj kodeka, liczba wysłanych, odebranych i zgubionych pakietów z próbkami głosowymi, zmienność opóźnienia przesyłania tych pakietów) – używane dla celów diagnostycznych w przypadku konieczności diagnozowania przez administratorów problemów z jakością transmisji głosu w systemie telekomunikacyjnym.
11. Urządzenie musi posiadać wbudowany system głośnomówiący (tzw. speakerphone), umożliwiający prowadzenie rozmowy bez podnoszenia słuchawki i działający w trybie full-dupleks
12. Urządzenie musi posiadać gniazdo USB z budżetem mocy 2,5W (prąd 500mA) w celu obsługi funkcji ładowania urządzeń przenośnych takich jak smartfony.

13. Urządzenie musi obsługiwać dodatkowy nowoczesny cyfrowy zestaw nagłowny wysokiej jakości dołączany do portu USB, a ponadto musi posiadać dedykowane gniazda audio in/out do podłączenia typowego komputerowego analogowego zestawu nagłownego. Nie jest dopuszczalne rozwiązanie, gdzie zestaw nagłowny dołącza się zamiast albo razem ze słuchawką na tym samym gnieździe.
14. Urządzenie musi posiadać co najmniej 5 przycisków kontekstowych, których funkcje zależą od stanu (np. inne, gdy nie ma połączenia, inne gdy jest połączenie, inne gdy jest połączenie przychodzące, inne gdy połączenie jest zawieszone).
15. Urządzenie musi posiadać co najmniej następujące dedykowane przyciski:

- przycisk dostępu do listy kontaktów,
- przycisk dostępu do poczty głosowej,
- przycisk dostępu do aplikacji biznesowych,
- przycisk zawieszenia połączenia,
- przycisk przekierowania połączenia,
- przycisk połączenia konferencyjnego.

16. przycisk sterujący głośnością (dający możliwość ustawienia głośności w słuchawce, w zestawie nagłownym oraz w trybie głośnomówiącym; osobno dla każdego z tych trybów)
17. Urządzenie musi posiadać co najmniej następujące dedykowane przyciski:

- przycisk Mute (wyłączenie mikrofonu),
- przycisk trybu Headset (rozmowa przez system nagłowny),
- przycisk trybu Speaker (rozmowa przez system głośnomówiący).

18. Urządzenie musi posiadać posiadać czterokierunkowy (góra/dół/lewo/prawo) przycisk nawigacyjny umożliwiający poruszanie się po różnych menu.
19. Urządzenie musi dawać dostęp do systemowej książki telefonicznej.
20. Urządzenie musi posiadać wbudowany przełącznik Ethernet, z dwoma portami 10/100/1000 Mb/s.
21. Port przełącznika urządzenia w kierunku przełącznika sieciowego powinien wspierać trunking 802.1Q celem odseparowania ruchu głosu i ruchu danych.
22. Transmisja głosu/obrazu oraz danych z komputera PC dołączonego do urządzenia muszą być przesyłane w dwóch różnych sieciach VLAN
23. Urządzenie musi zapewniać wsparcie dla protokołu sterującego SIP.
24. Urządzenie musi posiadać dwa niezależne banki do przechowywania dwóch wersji oprogramowania systemowego (firmware), w celu zminimalizowania przerwy w pracy urządzenia w przypadku konieczności aktualizacji firmware.
25. Urządzenie musi umożliwiać zasilanie go z sieci komputerowej LAN (ang. Power over Ethernet - PoE) zgodnie ze standardami IEEE 802.3af oraz 802.3at, a także z wykorzystaniem lokalnych zasilaczy (transformujących napięcie z sieci 230V). Musi wspierać dla PoE protokoły wykrywania: co najmniej Link Layer Discovery Protocol - Power over Ethernet (LLDP-PoE) lub równoważne.
26. Menu urządzenia musi być zrealizowane w języku polskim oraz angielskim, przy czym wymagane jest, aby możliwa była zmiana rodzaju języka menu w zależności od ustawień w profilu zalogowanego na nim użytkownika.
27. Urządzenie musi posiadać wbudowany interfejs radiowy Bluetooth 3.0 EDR przeznaczony do bezprzewodowego dołączenia słuchawek Bluetooth. Musi obsługiwać komunikację Bluetooth z urządzeniami zewnętrznymi w zakresie trybu głośnomówiącego HFP (ang. Hands-Free Profile) oraz wymiany kontaktów PBAP (ang. Phone Book Access Profile).

28. Urządzenie musi posiadać wbudowane gniazdo typu Kensington lub równoważne, pozwalające na zamocowanie linki zabezpieczającej przed kradzieżą.
29. Urządzenie musi obsługiwać aplikacje w języku XML, w tym aplikacje XML innych producentów
30. Urządzenie musi obsługiwać pobieranie oraz wymianę plików konfiguracyjnych oraz oprogramowania z systemu zarządzania połączeniami.
31. Urządzenie musi obsługiwać oprogramowanie (firmware) podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez system zarządzania połączeniami.
32. Urządzenie powinno być zarządzane centralnie poprzez system komunikacyjny Zamawiającego w zakresie co najmniej:

- pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych Zamawiającego,
- obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne Zamawiającego,
- możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU),
- możliwości zdalnego restartu urządzenia lub grupy urządzeń,
- możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego.

33. Urządzenie powinno być dostarczone z dedykowaną przystawką rozszerzającą programowalne klawisze szybkiego wybierania do 36.
34. Przystawka do telefonu musi posiadać duży, kolorowy ciekłokrystaliczny wyświetlacz, o rozdzielczości co najmniej 480 x 272 z 16-bitowa głębią koloru.
35. Wyświetlacz musi posiadać podświetlenie.
36. Przystawka do telefonu musi posiadać 18 fizycznych przycisków na linie z podświetlanymi przyciskami sygnalizującymi stan połączenia lub stan innej monitorowanej linii za pomocą kolorów: zielony - dostępny, pomarańczowy - zajęty, czerwony – linia współdzielona lub status „nie przeszkadzać”.
37. Musi mieć możliwość obsługi i monitorowania do 36 linii za pomocą przełączania stron na wyświetlaczu.
38. Musi mieć możliwość połączenia kaskady trzech przystawek obok siebie, pozwalających na obsługę łącznie 108 linii.
39. Musi posiadać funkcje czuwania podczas brak aktywności w celu oszczędzania energii. Musi mieć możliwość wyłączenia podświetlenia, wówczas we współpracy z telefonem następuje wyłączenie podświetlenia wyświetlacza przystawki oraz wyświetlacza telefonu.
40. Przystawka musi być zasilana z telefonu, do którego jest zamontowana jako rozszerzenie.
41. Każdy przycisk przystawki powinien mieć możliwość definiowania jako dodatkowa linia lub klawisz szybkiego wyboru.
42. Każdy klawisz musi mieć możliwość opisania przez informację wyświetloną na wyświetlaczu.

43. Przystawka musi posiadać regulację umożliwiającą ustawienie ekranu w co najmniej dwóch pozycjach, dopasowując kąt wyświetlacza przystawki i wyświetlacza telefonu zgodnie z preferencjami użytkownika.
44. Przystawka musi mieć kolor ciemny, identyczny z kolorem telefonu, do którego jest dołączana.
45. Wszystkie elementy rozwiązania muszą pochodzić od jednego producenta i być objęte wspólną gwarancją i serwisem producenta.

Telefon wideo IP, z kolorowym wyświetlaczem – EC6 (pozycja nr 14 z tabeli)

1. Urządzenie musi wspierać kodek audio szerokopasmowy zgodnie ze standardem G.722, przy czym słuchawka, mikrofon oraz głośnik aparatu powinny umożliwiać wykorzystanie możliwości tego kodeka tak by zapewnić wysoką jakość rozmowy telefonicznej.
2. Urządzenie powinno być dostarczone w kolorze białym.
3. Urządzenie musi wspierać kodeki audio co najmniej określone przez standardy G.711a, G.711μ i G.729a tak by umożliwić współpracę z telefonami IP starszych generacji, nie obsługującymi kodeków szerokopasmowych, a także rozwiązaniami systemów telekomunikacyjnych innych producentów.
4. Urządzenie musi wspierać kodeki audio działające zgodnie ze standardem iLBC (internet Low Bitrate Codec) oraz iSAC (internet Speech Audio Codec) – dla zapewnienia możliwości wykorzystania telefonów w placówkach objętych łączami o słabych lub niegwarantowanych parametrach jakościowych QoS.
5. Urządzenie musi realizować połączenia wideo poprzez kodowanie i dekodowanie strumienia wideo na bazie kodeka H.264 AVC.
6. Urządzenie musi umożliwiać kodowanie obrazu o wysokiej rozdzielczości (High Definition, HD) co najmniej HD720p, z prędkością nie mniejszą niż 24 klatki na sekundę.
7. Urządzenie musi posiadać duży, o przekątnej co najmniej 5 cali, kolorowy ekran wysokiej jakości (minimum 800x480 pikseli), umożliwiający jego wygodną obsługę, odczytywanie informacji i wywoływanie funkcji urządzenia oraz obsługujący wyświetlanie na nim ruchomego strumienia wideo.
8. Urządzenie musi posiadać wbudowaną kamerę wideo o rozdzielczości matrycy zapewniającej obsługę wideo (High Definition, HD) o jakości co najmniej HD 720p.
9. Urządzenie musi posiadać regulację umożliwiającą ustawienie go w co najmniej dwóch pozycjach, dopasowując kąt do preferencji użytkownika. Urządzenie musi mieć kolor ciemny.
10. Urządzenie musi zawierać co najmniej 5 przycisków z podświetleniem wbudowanym w przycisk, umożliwiających wybór linii oraz obserwację jej stanu (zajętość/dostępność), bądź też obserwację stanu linii innego urządzenia w systemie. Urządzenie musi umożliwiać zwiększenie liczby takich przycisków przez dołączenie do niego dodatkowych przystawek.
11. Urządzenie musi mieć możliwość doposażenia w dodatkowe przystawki zwiększające ilość takich fizycznych przycisków o co najmniej 54 przyciski.
12. W zakresie bezpieczeństwa urządzenie musi pozwalać na:

- zabezpieczenie komunikacji z serwerem sterującym za pomocą TLS,
- zabezpieczenie strumienia audio oraz wideo za pomocą sRTP.

13. Urządzenie musi mieć wbudowane oprogramowanie klienta VPN w celu szyfrowania transmisji.

14. Urządzenie musi na bieżąco w czasie trwania rozmowy umożliwiać wyświetlanie lokalnie na jego ekranie, a także zdalnie poprzez przeglądarkę internetową, informacji diagnostycznych o połączeniu (rodzaj kodeka, liczba wysłanych, odebranych i zgubionych pakietów z próbkami głosowymi, zmienność opóźnienia przesyłania tych pakietów) – używane dla celów diagnostycznych w przypadku konieczności diagnozowania przez administratorów problemów z jakością transmisji głosu w systemie telekomunikacyjnym.
15. Urządzenie musi posiadać wbudowany system głośnomówiący (tzw. speakerphone), umożliwiający prowadzenie rozmowy bez podnoszenia słuchawki i działający w trybie full-dupleks.
16. Urządzenie musi posiadać co najmniej dwa dedykowane gniazda typu USB. Co najmniej jedno gniazdo USB musi dysponować budżetem mocy 10W (prąd 2000mA) w celu obsługi funkcji szybkiego ładowania urządzeń przenośnych takich jak smartfony oraz tablety.
17. Urządzenie musi obsługiwać dodatkowy nowoczesny cyfrowy zestaw nagłowny wysokiej jakości dołączany do portu USB, a ponadto musi posiadać dedykowane gniazda audio in/out do podłączenia typowego komputerowego analogowego zestawu nagłownego. Nie jest dopuszczalne rozwiązanie, gdzie zestaw nagłowny dołącza się zamiast albo razem ze słuchawką na tym samym gnieździe.
18. Urządzenie musi posiadać co najmniej 5 przycisków kontekstowych, których funkcje zależą od stanu (np. inne gdy nie ma połączenia, inne gdy jest połączenie, inne gdy jest połączenie przychodzące, inne gdy połączenie jest zawieszone).
19. Urządzenie musi posiadać co najmniej następujące dedykowane przyciski:

- przycisk dostępu do listy kontaktów,
- przycisk dostępu do poczty głosowej,
- przycisk dostępu do aplikacji biznesowych,
- przycisk zawieszenia połączenia,
- przycisk przekierowania połączenia,
- przycisk połączenia konferencyjnego,
- przycisk sterujący głośnością (dający możliwość ustawienia głośności w słuchawce, w zestawie nagłownym oraz w trybie głośnomówiącym; osobno dla każdego z tych trybów).

20. Urządzenie musi posiadać co najmniej następujące dedykowane przyciski:
21. przycisk Mute (wyłączenie mikrofonu),

- przycisk trybu Headset (rozmowa przez system nagłowny),
- przycisk trybu Speaker (rozmowa przez system głośnomówiący).

22. Urządzenie musi posiadać czterokierunkowy (góra/dół/lewo/prawo) przycisk nawigacyjny umożliwiający poruszanie się po różnych menu.
23. Urządzenie musi dawać dostęp do systemowej książki telefonicznej.
24. Urządzenie musi posiadać wbudowany przełącznik Ethernet, z dwoma portami 10/100/1000 Mb/s.
25. Port przełącznika urządzenia w kierunku przełącznika sieciowego powinien wspierać trunking 802.1Q celem odseparowania ruchu głosu i ruchu danych.
26. Transmisja głosu/obrazu oraz danych z komputera PC dołączonego do urządzenia muszą być przesyłane w dwóch różnych sieciach VLAN.
27. Urządzenie musi posiadać wbudowany interfejs bezprzewodowy zgodny ze standardami 802.11a, 802.11b, 802.11g, 802.11n oraz 802.11ac, umożliwiający użytkowanie go w miejscach, gdzie z powodów technologicznych lub estetycznych byłoby niemożliwe lub niewskazane dołączanie do sieci LAN.
28. Urządzenie musi zapewniać wsparcie dla protokołu sterującego SIP.

29. Urządzenie musi posiadać dwa niezależne banki do przechowywania dwóch wersji oprogramowania systemowego (firmware), w celu zminimalizowania przerwy w pracy urządzenia w przypadku konieczności aktualizacji firmware.
30. Urządzenie musi umożliwiać zasilanie go z sieci komputerowej LAN (ang. Power over Ethernet - PoE) zgodnie ze standardami IEEE 802.3af oraz 802.3at, a także z wykorzystaniem lokalnych zasilaczy (transformujących napięcie z sieci 230V). Musi wspierać dla PoE protokoły wykrywania: co najmniej Link Layer Discovery Protocol - Power over Ethernet (LLDP-PoE) lub równoważne. Wraz z urządzeniem należy dostarczyć zasilacz oraz przewód zasilający.
31. Menu urządzenia musi być zrealizowane w języku polskim oraz angielskim, przy czym wymagane jest, aby możliwa była zmiana rodzaju języka menu w zależności od ustawień w profilu zalogowanego na nim użytkownika.
32. Urządzenie musi posiadać wbudowany interfejs radiowy Bluetooth 4.1 LE (Low Energy) EDR przeznaczony do bezprzewodowego dołączenia słuchawek Bluetooth. Musi obsługiwać komunikację Bluetooth z urządzeniami zewnętrznymi w zakresie trybu głośnomówiącego HFP (ang. Hands-Free Profile) oraz wymiany kontaktów PBAP (ang. Phone Book Access Profile).
33. Urządzenie musi posiadać wbudowane gniazdo typu Kensington lub równoważne, pozwalające na zamocowanie linki zabezpieczającej przed kradzieżą.
34. Urządzenie musi obsługiwać aplikacje w języku XML, w tym aplikacje XML innych producentów.
35. Urządzenie musi obsługiwać pobieranie oraz wymianę plików konfiguracyjnych oraz oprogramowania z systemu zarządzania połączeniami.
36. Urządzenie musi obsługiwać oprogramowanie (firmware) podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez system zarządzania połączeniami.
37. Urządzenie powinno być zarządzane centralnie poprzez system komunikacyjny Zamawiającego wzakresie co najmniej:

- pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych Zamawiającego,
- obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne Zamawiającego,
- możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU),
- możliwości zdalnego restartu urządzenia lub grupy urządzeń,
- możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego.

Telefon IP telekonferencyjny- EC7 - pozycja nr 15 z tabeli)

1. Musi być urządzeniem przeznaczonym w salach konferencyjnych do umieszczenia na stole konferencyjnym oraz umożliwiać prowadzenie rozmów w trybie głośnomówiącym.
2. Wsparcie dla kodeka szerokopasmowego zgodnie ze standardem G.722, przy czym słuchawka, mikrofon oraz głośnik aparatu powinny umożliwiać wykorzystanie możliwości tego kodeka tak, by zapewnić wysoką jakość rozmowy telefonicznej.
3. Musi posiadać wsparcie dla kodeków co najmniej określonych przez standardy G.711 i G.729a tak, by umożliwić współpracę z telefonami IP starszych generacji, nieobsługującymi kodeków szerokopasmowych, a także rozwiązaniami systemów telekomunikacyjnych innych producentów.

4. Urządzenie musi wspierać kodek audio wąskopasmowy działający zgodnie ze standardem iLBC – dla zapewnienia możliwości wykorzystania telefonów w placówkach objętych łączami o słabych lub niegwarantowanych parametrach jakościowych QoS.
5. Musi być urządzeniem wyposażonym w port sieciowy Ethernet 10/100Base-T umożliwiający podłączenie do sieci LAN.
6. Musi mieć możliwość zasilania z sieci komputerowej (802.3af) oraz z wykorzystaniem lokalnego zasilacza 230V.
7. Musi mieć możliwość zdefiniowania minimum 1 linii telefonicznej.
8. Musi posiadać graficzny, podświetlany wyświetlacz o rozdzielczości co najmniej 396 x 162 pikseli.
9. Układ głośnikowy urządzenia powinien realizować funkcje kontroli głośności (Automatic Gain Control), generację szumu (Comfort Noise Generation), wykrywanie ciszy (Voice Activity Detection), likwidację echa (Echo Suppression), dynamiczną redukcję szumu otoczenia (Dynamic Noise Reduction) o poziom co najmniej 9dB.
10. Musi mieć możliwość regulacji rozmowy oraz głośności dzwonka.
11. Musi mieć możliwość doboru sygnału dzwonienia poprzez zastosowanie własnych plików audio w formacie PCM w systemie sterowania połączeniami.
12. Musi umożliwiać podłączenie co najmniej dwóch dodatkowych mikrofonów dołączonych poprzez przewody do terminala w celu rozszerzenia zasięgu dźwięku przy zastosowaniu terminala w dużych salach konferencyjnych.
13. Musi umożliwiać podłączenie do zestawu dwóch mikrofonów bezprzewodowych w celu rozszerzenia zasięgu dźwięku przy zastosowaniu terminala w dużych salach konferencyjnych, gdzie prowadzenie przewodów do dodatkowych mikrofonów nie jest możliwe.
14. Musi umożliwiać dołączenie drugiego terminala w kaskadę, tworząc jedno logiczne urządzenie, w celu rozszerzenia zasięgu dźwięku przy zastosowaniu w bardzo dużych salach konferencyjnych.
15. Musi posiadać panel sterujący umożliwiający realizację poniższych funkcji poprzez naciśnięcie dedykowanych przycisków:

- klawiatura numeryczna do wprowadzania numeru tel. oraz innych danych,
- regulacja głośności,
- odebranie/zakończenie połączenia,
- wyciszenie mikrofonu.

16. Panel sterujący musi posiadać co najmniej 4 klawisze programowalne.
17. Musi wspierać standard markowania ruchu 802.1Q/p.
18. W zakresie bezpieczeństwa telefon musi umożliwiać możliwość identyfikacji w momencie dołączania do infrastruktury sieciowej za pomocą protokołu 802.1X EAP-FAST oraz EAP-TLS.
19. Dla zwiększenia bezpieczeństwa prowadzonych połączeń, telefon musi wspierać protokoły sRTP (szyfrowanie mediów) oraz TLS (szyfrowanie sygnalizacji).
20. Musi wspierać protokół sterujący SIP.
21. Musi spełniać następujące wymagania:

- Wyświetlanie nazwy i numeru dzwoniącego,
- Wizualizacja stanu aparatu, linii i połączenia,
- Podgląd połączeń nieodebranych,

- Automatyczne odbieranie połączenia przychodzącego,
- Funkcje telefonii takie jak: przekierowywanie połączeń, przełączenie (transfer) połączenia z konsultacją lub bez konsultacji, zawieszenie połączenia,
- Funkcja połączenia oczekującego oraz funkcję „nie przeszkadzać”,
- Funkcje książki telefonicznej,
- Sygnalizacja wiadomości głosowych,
- Możliwość tworzenia własnej listy wybierania skróconego.

22. Musi umożliwiać pracę aplikacji XML na wyświetlaczu telefonu.
23. Musi pobierać parametry wymagane do pracy w sieci automatycznie z systemu centralnego.
24. Musi posiadać oprogramowanie (firmware) zabezpieczone podpisem kryptograficznym producenta.
25. Menu telefonu musi być zrealizowane w języku polskim.
26. Telefon musi posiadać zestaw dwóch mikrofonów podłączonych przewodowo.

Wsparcie techniczne dla poszczególnych komponentów infrastruktury sieciowej, systemów zarządzania, kontroli i zwiększenia poziomu bezpieczeństwa sieci

Wymagane wsparcie techniczne na poszczególne produkty, wymaga obsługi na wszystkie komponenty systemu telefonii IP, aplikacje przez okres 3 lat od daty dostawy sprzętu i oprogramowania. Dodatkowy okres powinien być możliwy do dostarczenia, opcjonalnie.

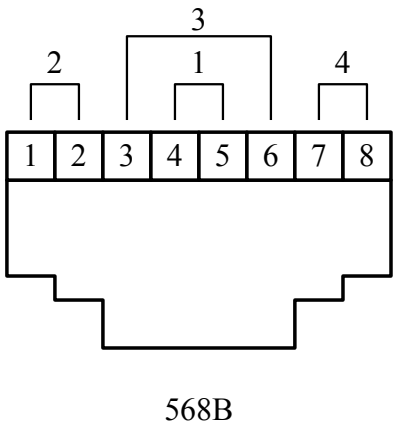
W ramach obsługi wsparcia technicznego zakłada się następujące parametry, dla wszystkich komponentów systemu telefonii IP i obsługi połączeń faksowych:

1. Obsługa w okresie 3 lat w trybie NBD (ang. Next Business Day), świadczone przez producenta danego elementu systemu telefonii IP.
2. Dostępna obsługa TAC (ang. Technical Assistance Center) świadczone przez producenta, dla wszystkich dostarczanych komponentów systemu, realizowana w trybie 8x5xNBD.
3. W ramach obsługi serwisowej zapewniony jest dostęp do nowych wersji oprogramowania dla poszczególnych produktów, aktualizacji poszczególnych funkcjonalności i do dokumentacji technicznej przez cały okres świadczenia usług wsparcia technicznego.
4. Wymiana uszkodzonego sprzętu odbywać się przez wymagany okres czasu w trybie NBD.
5. Dla systemów i oprogramowania wymagającego subskrypcji, zakłada się okres 3 lat świadczenie usługi aktualizacji, dostępnej dla poszczególnych systemów, realizowanej bezpośrednio przez producenta.
6. W ramach wsparcia technicznego zapewniony jest bezpośredni dostęp pracowników Szpitala, do wsparcia technicznego producenta danego komponentu sieciowego, systemu zarządzania itp.

4.1.3.3 Opis części pasywnej

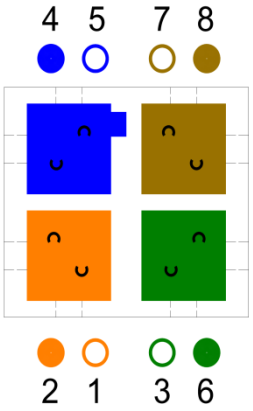
Sekwencja i polaryzacja

Poniższy rysunek przedstawia przyporządkowanie par kabla S/FTP do styków gniazd RJ45:



Nr pinu gniazda RJ45	Nr żyły kabla 4UTP	Kolor żyły
5	1	biało-niebieski
4	2	niebieski-biały
1	3	biało-pomarańczowy
2	4	pomarańczowo-biały
3	5	biało-zielony
6	6	zielono-biały
7	7	biało-brązowy
8	8	brązowo-biały

Poniższy rysunek przedstawia przyporządkowanie par kabla S/FTP do styków gniazd MATO (Multi Purpose Telecommunication Outlet)



Nr pinu gniazda MATO	Nr żyły kabla	kolor żyły
5	1	biało-niebieski
4	2	niebiesko-biały
1	3	biało-pomarańczowy
2	4	pomarańczowo-biały
3	5	biało-zielony
6	6	zielono-biały
7	7	biało-brązowy
8	8	brązowo-biały

Oplot kabla oraz metalizowaną folię stanowiącą ekran poszczególnych par należy w sposób przewidziany przez producenta podłączyć do ekranu gniazda RJ45/MATO oraz do uziemienia po stronie punktu dystrybucyjnego.

Połączenia pomiędzy szafami

Pomiędzy szafami w pomieszczeniu IT (serwerownia) w piwnicy (lokalizacja GPD oraz SA1-5 i SB1-5) a szafami PPD na poszczególnych kondygnacjach zostaną wykonane połączenia światłowodowe w postaci kabli 12 włóknowych OS2 zakończonych końcówkami LCD oraz zestawami po 4 kable S/FTP kat. 8.2 dla połączeń których długość < 30m, po 4 kable S/FTP kat. 7A dla połączeń których długość >30m – wszystkie zakończone gniazdami MATO 4P, kat.8.2.

Połączenia przedstawia schemat ideowy w części rysunkowej.

Pomiędzy szafami SB oraz SA zostaną wykonane połączenia w postaci kabli 24 włóknowych OS2 zakończonych końcówkami LCD/LCQ oraz zestawami po 6 kabli S/FTP kat. 8.2 dla połączeń których długość < 30m – wszystkie zakończone gniazdami MATO 4P, kat.8.2.

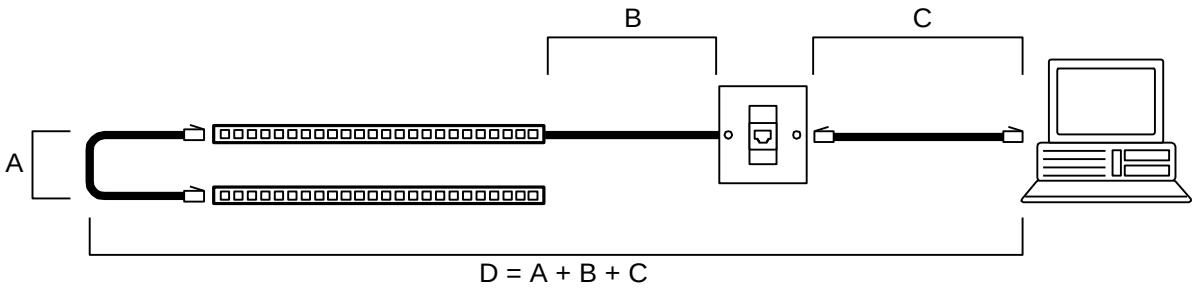
Przyjęto zasadę że oprócz podstawowego połączenia w topologii gwiazdy zostaną wykonane nadmiarowe połączenia do co najmniej dwóch sąsiednich Punktów Dystrybucyjnych.

Zasilanie poszczególnych szaf wg projektu elektrycznego. W projekcie przewidziano możliwość ręcznego przepięcia zasilania poszczególnych PPD pod inną sekcję zasilania, w przypadku serwisu bądź awarii urządzeń zasilających.

Okablowanie poziome

Do przełącznicy LAN należy doprowadzić kable S/FTP z poszczególnych PL. W okablowaniu poziomym pomiędzy gniazdem i punktem dystrybucyjnym maksymalna długość przebiegu kabla wynosi 90 m.

Wymagania instalacyjne dla przebiegów poziomych – zalecane długości linii.



Rys. Przedstawienie segmentów kabli.

	Maksymalna długość
A	nie więcej niż 6 m
A + C	łącznie 10 m
B	90 m
D	100 m

Należy szczególnie zwrócić uwagę na optymalizację tras kablowych do najdalej położonych PL, tak aby nie przekroczyć maksymalnej długości 90 m.

Oprócz standardowych zakończeń PL jako 1xRJ45 kat. 6A, na poziomie parteru oraz drugiego piętra w strefach PPD.0.1 i PPD.2.1 zostaną wykonane punkty multimedialne za pomocą światłowodu 4E9 oraz dwóch skrętek S/FTP min. 1500 MHz.

Piętrowe Punkty Dystrybucyjne będą umieszczone w szafach 47U 800x800. Standardowo będą to po dwie szafy na PPD, w przypadku PPD.0.1 i PPD.2.1 – trzy szafy ze względu na ilość okablowania i sprzętu aktywnego. Do pierwszej szafy zostaną doprowadzone kable związane z siecią LAN, do drugiej kable związane z sieciami bezpieczeństwa (SKD, CCTV, system parkingowy, BMS, windy, itp.)

Dla sieci LAN będą zastosowane kable S/FTP kat 7, dla sieci bezpieczeństwa kable U/FTP kat 6A, kabel kat 7 – żółte, kable kat 6A – niebieskie.

System szaf serwerowych i dystrybucyjnych

Szafy muszę spełniać najnowsze wydania norm ISO 11801:2002/Am1:2008+Am2:2010, EN 50173-1: 2011, EN 50173-2: 2008/ A1: 2011, EN 50174-1: 2010/A1: 2011, PN-EN 50310:2012, TIA/EIA-

568-B.2, PN/E 08106/EN 60529, EN-6297-3-100, PN-EN 41003, PN-EN 60529:2003, EIA-310-B i dyrektywami 73/23/EWG oraz 93/68/AWG.

Szafy muszą być produkowane zgodnie z systemem jakości ISO 9001 oraz ISO14001. Producent szaf musi spełniać wymagania dotyczące normy jakości w spawalnictwie DIN EN ISO 3834 poprzez posiadanie ważnego certyfikatu potwierdzającego pełne wymagania (poziom drugi): DIN EN ISO 3834-2.

Rama spawana stabilna, laserowo cięta z profili stalowych gr. min 1,5 mm o nośności przynajmniej 1500 kg, otworowana w każdej płaszczyźnie. Istnieje możliwość jednoczesnego zastosowania nóżek poziomujących oraz kół. Rama szafy z licznymi poziomymi oraz pionowymi otworami umożliwiającymi montaż elementów do organizacji okablowania oraz listew zasilających. Przykręcany dach wyposażony w min. 4 otwory 2U (dach do szafy szerokości 800mm posiada dodatkowe otwory poza płaszczyzną 19'' do wprowadzenia okablowania).

Szafa musi być w standardzie przystosowana do zabudowy zimnego/gorącego korytarza oraz pod montaż elementów rack typu: organizatory, panele, urządzenia aktywne.

Panel organizacyjny pionowy musi posiadać funkcjonalność zwiększenia przestrzeni rakowej szafy minimalnie o 3U.

Istnieje możliwość dowolnej konfiguracji przepustów kablowych oraz paneli wentylacyjnych.

Profil ramy wykorzystywany również w szafach szczelnych IP 55 i więcej.

Spód i sufit szafy otwarty z możliwością indywidualnej konfiguracji poprzez zastosowania zaślepek z przepustami kablowymi, panelami wentylacyjnymi, wkładkami filtracyjnymi.

4 belki montażowe z możliwością beznarzędziowego przesuwu (system beznarzędziowy nie obniża obciążalności szafy), każda z zaznaczoną wysokością U (numeryczny opis).

Istnieje możliwość rozstawu od 19'' do 21'', możliwość dzielenia tylnych belek montażowych w poziomie na dwie niezależne sekcje o różnych rozstawach głębokości.

Drzwi przednie oraz tylne z perforacją 82%, oraz powierzchnią perforacji 69%. Możliwość montażu prawo i lewostronnego oraz beznarzędziowego demontażu/montażu drzwi. Drzwi w standardzie przystosowane pod montaż zamków elektromagnetycznych, wyposażone są w metalowy kanał kablowy do prowadzenia kabla po obrzeżach. Możliwość otwarcia drzwi o 225'. W standardzie wyposażone z zamek 4 punktowy.

Możliwość dzielenia ścian bocznych w poziomie na 2, 3 lub 4 sekcje, ściany z blachy stalowej, zdejmowane, mocowane przy pomocy na zatrzask z możliwością jednoczesnego zamknięcia na klucz.

Wszystkie szafy przygotowane do zabudowy typu kiosk.

Wszystkie szafy należy wyposażyć we wszystkie prowadnice/maskownice kabli poziomych i pionowych na całej wysokości szafy według rysunków z projektu (nawet jeśli szafa jest pusta).

System szaf serwerowych musi być dostosowany do instalacji systemu kanałów teleinformatycznych montowanych bezpośrednio na dachu szaf. Producent musi posiadać taki system kanałów nasufitowych w ofercie.

W szafie należy zamontować listwę uziemiającą i zapewnić odpowiednie połączenie galwaniczne pomiędzy uziemieniem i elementami metalowymi w szczególności panelami ekranowanymi.

Szafy muszą posiadać pisemne potwierdzenie możliwości instalacji sprzętu IT wiodących producentów takich jak: serwery Dell, IBM, HP, Fujitsu, macierze NetApp, EMC, Hitachi, Dell, IBM, przełączniki Brocade, Cisco, Extreme, F5 itp.

W przypadku stosowania paneli wentylacyjnych dla szaf umiejscowionych w pomieszczeniach biurowych należy zachować wymagania normy PN-N-01307:1994. Dla pomieszczeń gdzie jest wykonywana bardzo intensywna koncepcyjna praca umysłowa należy nie przekraczać poziomu 40 dB, a w standardowych pomieszczeniach biurowych poziomu 55dB do 65 dB.

Zabudowa serwerowa typu kiosk

Kiosk będzie składał się 10 szaf RACK 4DC 47U 800x1200 zamykanych układem mechanicznych drzwi przesuwnych z jednej strony oraz ścianą pełną od tyłu. Celem zapewnienia odpowiedniej wentylacji i przepływu powietrza w szafach należy stosować drzwi przednie perforowane, drzwi tylne dwuskrzydłowe perforowane. Szafy należy wyposażyć w komplet maskownic pionowych i poziomych oraz zaślepek wolnych przestrzeni zgodnie z zestawieniem materiałowym oraz rysunkami elewacji szaf celem zapewnienia prawidłowej cyrkulacji powietrza i nie mieszania się stref zimnych i ciepłych w przestrzeni szafy. Pomiędzy szafami zostaną zainstalowane urządzenia klimatyzacji precyzyjnej. Projektowane jest rozwiązanie ciepłego korytarza wewnątrz kiosku oraz zimnej strefy poza kioskiem. Montaż urządzeń odbywać się będzie od strony zimnej.

Szafy serwerowe muszą zapewniać kompatybilność oraz możliwość wykonania pełnej zabudowy z urządzeniami międzyszafowymi.

Drzwi automatyczne do kiosku należy podpiąć do centrali SUG w serwerowni. Powinny się automatycznie otworzyć w przypadku wyzwolenia środka gaśniczego.

Drzwi szaf serwerowych należy wyposażyć w wkładki umożliwijace ich otwieranie tylko przy pomocy dedykowanego klucza. Klucze do szaf należy przekazać, np. kierownikowi działu IT.

System tras kablowych

Zaleca się wykonanie odseparowanych tras kablowych dla instalacji teleinformatycznej miedzianej i światłowodowej poprzez zastosowanie dedykowanych kanałów kablowych montowanych bezpośrednio na dachach szaf serwerowych oraz łączących poszczególne rzędy szaf miedzy sobą minimum w dwóch torach równoległych:

System szaf serwerowych musi być dostosowany do instalacji systemu kanałów teleinformatycznych montowanych bezpośrednio na dachu szaf. Producent musi posiadać taki system kanałów nasufitowych w ofercie. Tego typu rozwiązanie gwarantuje prawidłowe rozprowadzenie okablowania pomiędzy szafami oraz redukcję ryzyka wystąpienia przerwy w połączeniach oraz zredukowanie ryzyka przerwania połączenia w sytuacji serwisu innych systemów we wspólnych trasach kablowych.

System koryt nad kioskiem należy połączyć z projektowanym systemem tras kablowych teletechnicznych budynku.

Zarządzalne listwy zasilające

Ze względu na konieczność monitorowania zasilania oraz środowiska w szafach należy zastosować zarządzalne listwy zasilające z monitoringiem środowiska. Listwy należy zintegrować z systemem BMS po protokole SNMP. Minimalne wymagania:

- Listwa ma zapewniać komunikację i wysyłanie alarmów poprzez wieloużytkownikowy interfejs webowy, e-mail do administratorów, trapy SNMP.
- Listwa ma zapewniać zarządzanie stanem (włączone/wyłączone) każdego wyjścia.
- Listwa ma zapewniać zdalny monitoring parametrów m.in. napięcie, obciążenie, Pobór mocy, zużycie energii, stany czujników, odczyt stanu gniazda (włączone/wyłączone) dla poszczególnego gniazda, fazy i całej listwy.
- Listwa ma być wyposażona w wyświetlacz i dwa przyciski do przełączania pomiędzy ekranami wyświetlacza.
  Listwa ma być wyposażona w zintegrowany moduł monitoringu parametrów środowiska. Moduł parametrów środowiska ma umożliwiać w standardzie podłączenie czujnika temperatury i wilgotności oraz wyprowadzenia sygnału alarmowego. Czujniki mają być podłączane do dedykowanych portów w standardzie RJ11.
- Listwa ma zapewniać alarmy systemowe (po podpięciu czujników): obecności dymu, obecności wody, otwarcia drzwi lub osłon bocznych szafy.

- Listwy mają mieć możliwość spięcia łańcuchowego w grupę do 4 listew w celu zarządzania i monitorowania grupy przy wykorzystaniu jednego adresu IP.
- Listwa ma zapisywać wszystkie zdarzenia alarmowe w logach w wewnętrznej pamięci.
- Listwa ma mieć możliwość restartu poszczególnych liczników zużycia energii (kWh).

Listwy musza być kompatybilne i musząc pozwalać na integrację z zewnętrznym oprogramowaniem do integracji i wizualizacji typu system automatyki serwerowni.

Dla szaf serwerowych SA i SB przewiduje się po dwie takie listwy, dla szaf dystrybucyjnych PPD po jednej na szafę.

Multimedialny moduł MATO

Wieloaplikacyjne gniazdo telekomunikacyjne MATO (Multi-application Telecommunications outlet) przeznaczone jest dla instalacji teleinformatycznych i multimedialnych. Wykonane w całości z metalu w konstrukcji jednoczęściowej, zapewniającej pełne ekranowanie 360°na poziomie obudowy oraz na poziomie każdej pary. Ciągłość ekranu na poziomie całej skrętki i na poziomu pary. Moduł ten spełnia wymagania dla kategorii 8.2.

Charakterystyka produktu:

- Złącze 2 x Faston 2,8mm.
- Dopuszczalny przekrój żył: AWG 22.
- Gniazdo 4-parowe.
- Zgodność z wymaganiami kompatybilności elektromagnetycznej EMC.
- Pełne ekranowanie 360° na poziomie gniazda i poszczególnych par.
- Złącze zapewniające połączenia gazoszczelne odporne na korozję i zanieczyszczenia.
- Moduł bez płytki drukowanej.
- Kompatybilny zarówno z kablem typu drut oraz linka.
- Pełna zgodność PoE / PoE + ze standardem IEEE 802.3af i IEEE 802.3at.

Właściwości fizyczne i mechaniczne:

- Gabaryty: 36 x 14 x 17 mm.
- Obudowa: Zn (cynk).
- Powierzchnia: Cu/Ni (miedź/nikiel).
- Styki: CuBe2 / Ag 0,8µm (miedź/beryl / srebro).
- Ilość cykli wpięcia/wypięcia wtyków do gniazda: >750.
- Temperatura pracy: -10°C do 60°C.

Właściwości elektryczne i transmisyjne:

- Rezystancja styku: 4,3 MΩ
- Rezystancja izolacji: >500 MΩ
- Dopuszczalne obciążenie prądowe: 1,5 A
- Impedancja sprzężeniowa: 10 MHz < 80 MΩ
- Pasmo przenoszenia: do 2300 MHz
- Tłumienność złącza: >88 dB

- Minimalny NEXT: 80dB / 2300 MHz

Standardy:

- Kat 7A zgodne z normą ISO/IEC 60603-7-71
- KL FA zgodne z normą ISO/IEC 11801 i EN 50173, 2.
- Multi-application Telecommunications outlet MATO ISO/IEC 15018
- Multi-application Telecommunications outlet MATO PN-EN 50173-4
- PN-EN 50173
- ANSI/TIA-568
- ISO/IEC 61076-3-104 2GHz Ed. 3.0
- EN 55022 (Klasa B)
- EN 50081
- EN 50082

Multi-application Telecommunications outlet MATO musi gwarantować obsługę wielu aplikacji zarówno kanałów ICT jak I BCT.

Wieloaplikacyjne gniazdo telekomunikacyjne MATO BKT.NL.4P musi gwarantować dowolny podział usług, transmisję aplikacji, podłączenia urządzeń z różnymi interfejsami min.: CATV-IEC, SAT-F, RJ45, RJ11, SCART, CINCH, Component Video, VGA, DVI, HDMI, USB, B&O, Bose, Revox.

Transmisja różnych aplikacji musi być realizowana poprzez specjalistyczne kable krosowe dostosowane dla każdej z żądanych aplikacji.

Multi-application Telecommunications outlet musi gwarantować transmisje minimalne 10Gigabit. Ethernet zdefiniowana dla kategorii 7A oraz możliwość transmisji 25 oraz 40 Gigabit Ethernetu.

Ekranowany moduł RJ45 kategorii 6A

Moduł RJ45 musi być wykonany w standardzie Keystone Jack, co pozwala na montaż w każdym dostępnym osprzęcie. Moduł RJ45 powinien zapewnić uniwersalność rozwiązania (taki sam moduł po stronie gniazda i po stronie panela krosowego modularnego). Moduł RJ45 musi posiadać możliwość zrobienia zarówno beznarzędziowego, narzędziowego oraz wielokrotnego użytku - pozwalać na demontaż z kabla skrętkowego a następnie powtórne zaterminowanie. TYP modułu RJ45 musi być taki sam dla wszystkich możliwych w danym systemie kategorii (kat5, kat6, kat6A) i technologii (ekranowanej i nieekranowanej) – (Jeden standard, jeden typ dla rozwiązania nieekranowanego i ekranowanego bez względu na kategorię). Moduł RJ45 musi posiadać kolorystyczne wyróżnienia kategorii dla której jest dedykowany.

Moduł RJ45 musi posiadać trwałe oznaczenie kategorii dla której jest dedykowany, logo producenta i logo systemu.

Moduł RJ45 Keystone JACK musi posiadać minimum jeden certyfikat notyfikowanego instytutu badawczych (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2(2011-06), EN 50173-1((2011-09), ANSI/TIA-568-C.2 (2009-08)} dla potwierdzenia spełniania parametrów.

Certyfikatów musi potwierdzać spełnianie następujących norm i standardów: IEC 60603-7-51, IEC 60512-27-100, IEC60512-99-001:2012, potwierdzać spełnienie procedury badawczej RE-EMBEDDED oraz potwierdzać kompatybilność z transmisją Power over Ethernet Plus (PoE+).

Moduł RJ45 Keystone JACK musi posiadać kolorową etykietę wskazującą rozprowadzenie żył skrętki w złączach IDC wg schematu T568A lub T568B. Podczas instalacji należy zastosować schemat T568B.

Adapter kątowy 2xRJ45 (45/45)

Punkt logiczny należy zbudować w oparciu o płytę czołową kątową z danej serii jaka została wybrana do osprzętu typu gniazda elektryczne i logiczne.

Zastosowanie adaptera kątowego wymusza prawidłowe ułożenie kabla skrętkowego w puszce pod lub natynkowej w postaci łagodnego wyprowadzenia skrętki w górę bez konieczności nadmiernego załamania, które może spowodować pogorszenie lub utratę prawidłowych parametrów transmisyjnych.

Panel krosowy dedykowany dla połączeń klasy FA

- Uniwersalny panel 19" dla modułów MATO i RJ45
- Zintegrowana półka kablowa umożliwiająca przymocowanie kabla,
- Metalowa konstrukcja zapewniająca galwaniczne połączenie z ekranami modułów,
- Styk do podłączenia uziemienia,
- Kolor: czarny (RAL 9005),
- Gabaryty: 1U (482,6 x 44 mm).

Zgodność z odpowiednimi wymaganiami zawartymi w normach:

- IEC 60297-3-100
- PN-EN 50173-1
- EN 50173-1
- ISO/IEC 11801
- ANSI/TIA-568-C.2

Kabel instalacyjny kategorii 7 SFTP

Dla punktów sieci LAN.

Okablowanie miedziane ma być prowadzone 4-parowym podwójnie ekranowanym kablem typu S/FTP (PiMF) kat.7 (wymagane oznaczenie na kablu). Kable wykonane w technologii trudnopalnej (LSZH – Low Smog Zero Halogen); FRNC (ang. Flame Retardant Non Corrosive), zgodnie z normą IEC 60754-2.

Kabel musi posiadać trwałe rozróżnienie kolorystyczne dedykowane dla kategorii.

Na kablu musi być naniesiony (na całej długości) indeks producenta, dokładny opis kategorii oraz sposobu ekranowania lub braku (X/XTP) oraz NVP.

Skrętka teleinformatyczna musi posiadać minimum jeden certyfikat niezależnego instytutów badawczych (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2(2011-06), IEC 61156-5 Ed.2.1 (2012-12), ANSI/TIA-568-C.2 (2009-8)} dla potwierdzenia spełniania parametrów.

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

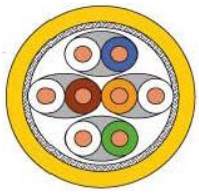
- w postaci jednostronnie laminowanej folii aluminiowej AL/PET. W kablu powinny być cztery taśmy ekranujące. Każda z nich powinna obejmować jedną parę, tak aby każdej z nich zapewnić pełne ekranowanie względem trzech sąsiednich (w celu redukcji oddziaływań miedzy parami).
- w postaci wspólnej siatki okalającej dodatkowo wszystkie pary (skręcone razem między sobą) – w celu redukcji wzajemnego oddziaływania kabli pomiędzy sobą.

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

Charakterystyka kabla ma uwzględniać odpowiedni margines pracy, tj. pozytywne parametry transmisyjne do min.690MHz dla kabla kat.7.

Opis konstrukcji:

Opis	Kabel S/FTP (PiMF) 695 MHz
Zgodność z normami	ISO/IEC 11801:2002 wyd. II, ISO/IEC 61156-5:2002, EN 50173-1:2011, EN 50288-3-1, TIA/EIA 568-B.2 (parametry kategorii 7), IEC 60332-1, IEC 60754-2; IEC 61034
Średnica przewodnika	drut 23 AWG (Ø 0,56 mm)
Liczba par kabla	4 (8 przewodów)
Średnica zewnętrzna kabla	6,9 mm
Minimalny promień gięcia	30mm
Waga	50,2 kg/km
Temperatura pracy	-20ºC do +60ºC
Temperatura podczas instalacji	0ºC do +50ºC
Osłona zewnętrzna	FRNC, kolor żółty
Ekranowanie par	laminowana folia aluminiowa
Ogólny ekran	plecionka miedziana, cynowana



Rys. Przekrój kabla S/FTP (PiMF)

Charakterystyka elektryczna – wartości typowe:

Pasmo przenoszenia (robocze)	690MHz
Pasmo przenoszenia max.	1000MHz
Impedancja 1-600 MHz:	100 ±5 Ohm
NVP	75%
Opóźnienie	500ns/100m
Tłumienie:	52,5dB przy 695MHz;
NEXT	80dB przy 695MHz
PSNEXT	77dB przy 695MHz,
PSELFEXT	38dB przy 695MHz;
RL:	19dB przy 695MHz,
ACR:	27dB przy 695MHz
Rezystancja izolacji	5 GOhm min. /km
Rezystancja przewodnika	145 Ohm max. /km
Pojemność wzajemna	44 nF/km dla 800 Hz
Tłumienie sprzężeniowe	≥80 dB

Kabel instalacyjny kategorii 7A SFTP 1500

Dla połączeń pomiędzy Punktami Dystrybucyjnymi których odległość > 30m oraz dla punktów multimedialnych.

Okablowanie miedziane ma być prowadzone 4-parowym podwójnie ekranowanym kablem typu S/FTP (PiMF) kat.7A (wymagane oznaczenie na kablu). Kable wykonane w technologii trudnopalnej; LSHF (LSOH), zgodnie z normą IEC 60754-2.

Kabel musi posiadać trwałe rozróżnienie kolorystyczne dedykowane dla kategorii.

Na kablu musi być naniesiony (na całej długości) indeks producenta, dokładny opis kategorii oraz sposobu ekranowania lub braku (X/XTP) oraz NVP.

Skrętka teleinformatyczna musi posiadać minimum jeden certyfikat niezależnego instytutów badawczych (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2((2011-06)), EN 50173-1:2011, IEC 61156-5 Ed.2.1, EN 50288-9-1:2012, ANSI/TIA 568-C.2, IEC 60332-1-2, IEC 61034-1, IEC 61034-2.1, IEC 60754-2, EMC 9 dla potwierdzenia spełniania parametrów.

Skrętka teleinformatyczna powinna umożliwiać transmisję 25GbE zgodnie z zaleceniami ISO/IEC 11801-9905 Installed Cabling to Support 802.3bq 25GBASE-T

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

- w postaci jednostronnie laminowanej folii aluminiowej AL/PET w kablu powinny być dwie taśmy ekranujące. Każda z nich powinna obejmować dwie pary, tak aby każdej z nich zapewnić pełne ekranowanie względem trzech sąsiednich (w celu redukcji oddziaływań miedzy parami).
- w postaci wspólnej siatki okalającej dodatkowo wszystkie pary (skręcone razem między sobą) – w celu redukcji wzajemnego oddziaływania kabli pomiędzy sobą.

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

Charakterystyka kabla ma uwzględniać odpowiedni margines pracy, tj. pozytywne parametry transmisyjne do min.1500MHz dla kabla kat.7A.

Opis konstrukcji:

Opis:	Kabel S/FTP (PiMF) 1500 MHz
Zgodność z normami:	ISO/IEC 11801:2002 wyd. II, EN 50173-1:2011, ISO/IEC 61156-5:Amd1, TIA/EIA 568-C.2, EN 50288-9-1:2012 IEC 60332-1; IEC 61034-1, IEC 61034-2, IEE802.3at
Średnica przewodnika:	drut 23 AWG (Ø 0,62 mm)
Liczba par kabla	4 (8 przewodów)
Średnica zewnętrzna kabla	8,3 mm
Minimalny promień gięcia	33 mm
Waga	62 kg/km
Temperatura pracy	-20ºC do +60ºC
Temperatura podczas instalacji	0ºC do +50ºC
Osłona zewnętrzna:	LSHF, LSOH, melonowo-żółty RAL 1028

Ekranowanie par:	laminowana folia aluminiowa
Ogólny ekran:	plecionka miedziana, cynowana

Rys. Przekrój kabla S/FTP (PiMF)

Charakterystyka elektryczna – wartości typowe:

Pasmo przenoszenia (robocze)	1000MHz
Pasmo przenoszenia max.	1500MHz
Impedancja 1-100 MHz:	100 ±5 Ohm
NVP	79%
Opóźnienie	450ns/100m
Tłumienie:	66dB przy 1500MHz;
NEXT	80dB przy 1500MHz;
PSNEXT	77dB przy 1500MHz;
PSACR-N	11dB przy 1500MHz;
RL:	15dB przy 1500MHz;
ACR-N:	14dB przy 1500MHz;
Tłumienie sprzężeniowe	≥80 dB

Kabel instalacyjny kategorii 8.2 S/FTP 2000

Dla połączeń w pomieszczeniu IT w piwnicy pomiędzy szafami SA, SB i GPD oraz dla połączeń pomiędzy PPD których odległość < 30m.

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 6,4mm (co determinuje maksymalną średnicę żyły na 22AWG). Nie dopuszcza się kabli o większej średnicy zewnętrznej.

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

- w postaci jednostronnie laminowanej folii aluminiowej AL/PET w kablu powinny być cztery taśmy ekranujące. Każda z nich powinna obejmować jedną parę, tak aby każdej z nich zapewnić pełne ekranowanie względem trzech sąsiednich (w celu redukcji oddziaływań miedzy parami).
- w postaci wspólnej siatki okalającej dodatkowo wszystkie pary (skręcone razem między sobą) – w celu redukcji wzajemnego oddziaływania kabli pomiędzy sobą.

Taka konstrukcja pozwala osiągnąć najwyższe parametry transmisyjne, zmniejszenie przesłuchu NEXT i PSNEXT oraz zmniejszyć poziom zakłóceń od kabli sąsiednich i elektrycznych. Pozwala także w dużym stopniu poprawić odporność na zakłócenia zarówno wysokich, jak i

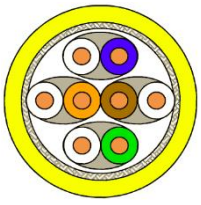
niskich częstotliwości. Kabel musi spełniać wymagania stawiane komponentom przez najnowsze obowiązujące specyfikacje.

Charakterystyka kabla ma uwzględniać odpowiedni margines pracy, tj. pozytywne parametry transmisyjne do min. 2000MHz dla kabla nowej kategorii kat.8.2.

Kabel instalacyjny ekranowany 4-parowy przeznaczony do instalacji teleinformatycznych i multimedialnych.

Opis konstrukcji:

Opis:	Kabel S/FTP (PiMF) 2000 MHz
Zgodność z normami:	ISO/IEC 11801:2002 wyd. II , , EN 50173-1, EN 50288-9-1 IEC 61156-5; IEC 61156-9 (46C/989/CD) PoE: IEEE 802.3af; IEEE 802.3at; IEEE 802.3bt
Średnica przewodnika:	drut 22 AWG (Ø 0,64 mm)
Liczba par kabla	4 (8 przewodów)
Średnica zewnętrzna kabla	8,5 mm
Minimalny promień gięcia	4xD
Waga	80 kg/km
Temperatura pracy	-20ºC do +60ºC
Temperatura podczas instalacji	0ºC do +50ºC
Osłona zewnętrzna:	LSHF-FR, żółty RAL 1021
Ekranowanie par:	laminowana folia aluminiowa PiMF
Ogólny ekran:	plecionka miedziana, cynowana



Przekrój kabla S/FTP (PiMF)

Charakterystyka elektryczna – wartości typowe:

Pasmo przenoszenia (robocze)	2000MHz
Pasmo przenoszenia max.	2000MHz

Impedancja 100 MHz:	100 ±5 Ohm
NVP	73%
Opóźnienie	20ns/100m
Tłumienie: (dB/100m)	88,4dB przy 2000MHz;
NEXT	70dB przy 2000MHz
PSNEXT	67dB przy 2000MHz,
PS-ACR-F	47dB przy 2000MHz;
RL:	15dB przy 2000MHz,
ACR: (dB/100m)	- 18,4dB przy 2000MHz
Rezystancja izolacji	5 GOhm min. /km
Rezystancja przewodnika	130 Ohm /km
Pojemność wzajemna	43 nF/km dla 800 Hz
Tłumienie sprzężeniowe	≥85 dB

Kabel instalacyjny kategorii 6A U/FTP

Dla punktów sieci bezpieczeństwa.

Okablowanie miedziane ma być prowadzone 4-parowym ekranowanym kablem typu U/FTP kat.6A (wymagane oznaczenie na kablu). Kable wykonane w technologii trudnopalnej (LSZH – Low Smog Zero Halogen) zgodnie z normą IEC 60754-2-1; LSHF (ang. Low Smoke Halogen Free), zgodnie z normą IEC 60332-1-2, IEC61034-2, IEC 61034-2 (potwierdzenie musi mieć miejsce w certyfikacie niezależnego akredytowanego laboratorium badawczego).

Kabel musi posiadać trwałe rozróżnienie kolorystyczne dedykowane dla kategorii.

Na kablu musi być naniesiony (na całej długości) indeks producenta, dokładny opis kategorii oraz sposobu ekranowania lub braku (X/XTP) oraz NVP.

Skrętka teleinformatyczna musi posiadać minimum jeden certyfikat niezależnego instytutów badawczych (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2, EN 50173-1:2011, ANSI/TIA 568-C.2,IEC 61156-5 Ed.2.1, EN 50288-10-1:2012, IEC 60332-1-2, IEC 61034-2.AMD1, IEC 61034-1, IEC 60754-2, EMC 7 dla potwierdzenia spełniania parametrów.

Instalacja ma być poprowadzona ekranowanym kablem konstrukcji U/FTP z osłoną zewnętrzną trudnopalną. Ekran takiego kabla ma być zrealizowany:

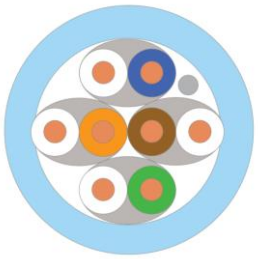
- kable powinny być cztery taśmy ekranujące (jednostronnie laminowanej folii aluminiowej AL/PET); każda z nich powinna obejmować jedną parę, tak aby każdej z nich zapewnić pełne ekranowanie względem trzech sąsiednich (w celu redukcji oddziaływań miedzy parami). Drut drenażowy AWG26 cynowany prowadzony wzdłuż konstrukcji kabla.

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

Charakterystyka kabla ma uwzględniać odpowiedni margines pracy, tj. pozytywne parametry transmisyjne do min. 585 MHz dla kabla kat.6 A.

Opis konstrukcji:

Opis:	Kabel U/FTP 585 MHz
Zgodność z normami:	EN 50173-1, ISO/IEC 11801:2002 wyd. II, ISO/IEC 61156-5:2002, EN 50288-5-1, TIA/EIA 568-B.2, IEC 60332-1-2, IEC61034-1, IEC 61034-2
Średnica przewodnika:	drut 23 AWG (Ø 0,55 mm)
Liczba par kabla	4 (8 przewodów)
Średnica zewnętrzna kabla	7,3 mm
Minimalny promień gięcia	35mm
Waga	45,0 kg/km
Temperatura pracy	-20ºC do +60ºC
Temperatura podczas instalacji	0ºC do +50ºC
Osłona zewnętrzna:	LSHF, kolor niebieski
Ekranowanie par:	laminowana folia aluminiowa



Rys. Przekrój kabla F/FTP

Charakterystyka elektryczna – wartości typowe:

Pasmo przenoszenia (robocze)	500MHz
Pasmo przenoszenia max.	585MHz
Impedancja 1-100 MHz:	100 ± 5 Ohm
NVP	75%
Opóźnienie	500ns/100m
Tłumienie:	43dB przy 500MHz;
NEXT	86dB przy 500MHz
PSNEXT	83dB przy 500MHz,
PSELFEXT	58dB przy 500MHz;
RL:	22dB przy 500MHz,
ACR:	43dB przy 500MHz
Rezystancja izolacji	5 GOhm /km

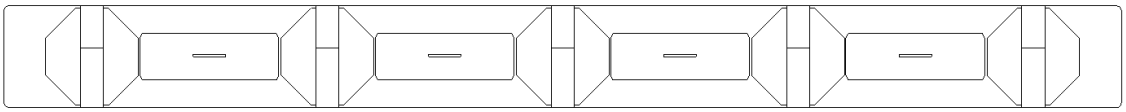
Pojemność wzajemna	45 nF/km dla 800 Hz

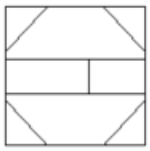
Modularny panel krosowy 24xRJ45 1U

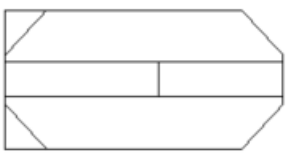
Kable należy zakończyć na 19", modularnym na 24xRJ45, ekranowany, 1U, czarny, na moduły Keystone, ekranowane, Kat.6A; Pozwalają na montaż modułów ekranowanych i nieekranowanych od kategorii 5e do 7A oraz adapterów światłowodowych lub gniazd/insertów typu F (rozwiązanie otwarte niezależne od kategorii, technologii, rodzaju usługi/aplikacji), co pozwala uzyskać zwiększone upakowanie złącz w szafie RACK w szczególności zastosowania pojedynczych połączeń światłowodowych (producent musi posiadać kable światłowodowe z fabrycznie zarobionymi złączami światłowodowymi o dolnym interfejsie). Panele krosowe muszą posiadać trwałe oznaczenie logo producenta i logo systemu oraz pole opisowe. Panel musi posiadać zintegrowana półkę kablową umożliwiającą przymocowanie kabli za pomocą opasek. Metalowa konstrukcja zapewnia galwaniczne połączenie z ekranami modułów oraz posiadać przewód uziemienia. Kolor czarny RAL 9005.

Poziomy organizator kabli 1U 19” z tworzywa sztucznego o podwyższonej elastyczności

W celu zapewnienia użytkownikowi komfortowego dostępu do każdego łącza tak, aby mógł w pełni zapanować nad wszystkimi elementami całego pasywnego systemu okablowania oraz zachować porządek ułożenia kabli nawet w trakcie reorganizacji, które są częścią użytkowania sieci, projekt uwzględnia zastosowanie dodatkowych elementów organizacyjnych. Zastosowane elementy prowadzące, gwarantują minimalny promień zagięcia zainstalowanych kabli połączeniowych (miedzianych lub światłowodowych), zaś kątowa konstrukcja narożnych prowadnic redukuje naprężenia kabli i ich zagęszczenie oraz pozwala na lepsze zarządzanie kablami z uwzględnieniem prowadzenia kabli krosowych. Powoduje to, że można znacznie ograniczyć potrzebę stosowania wieszaków i organizatorów poziomych (które zabierają wysokość montażową „U” w szafie), a tym samym znacząco podnieść pojemność i gęstość połączeń w punkcie dystrybucyjnym.







Kabel krosujący kat. 6A S/FTP

W celu zapewnienia wysokiej jakości połączeń wymaga się zastosowania kabli krosowych S/FTP Kat.6A (10Gbit-500MHZ) ze złączami RJ45 zaciskanymi mechanicznie (nie dopuszcza się kabli krosowych zalewanych), wykonane na kablu typu linka min. kat.6A.

Parametry minimalne:

- Złącze RJ45, ekranowane, TIA/EIA 568B.
- Osłonka w kolorze kabla.
- Trwałość: min. 200 cykli
- Eletryczne parametry pracy: max 250V / 2A
- Wytyrzymałość elektryczna: 1000 V/60s
- Częstotliwość pracy – min. 500 MHz.
- Tworzywo: UL.94V-2
- Materiał wykończenia PINów – złoto: 50µm
- Kabel - S/FTP kat. 7, 600 MHz AWG 26 LSOH, 4x2x0,42

Kabel patchcordowy musi posiadać minimum jeden certyfikat niezależnego instytutów badawczych (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2((2011-06)), EN 50173-1:2011, IEC 61156-6 amd.1, EN 50288-6-1:2013, ANSI/TIA 568-C.2, IEC 60332-1-2, IEC 61034-2.AMD1, IEC 61034-1, IEC 60754-2, EMC 10 dla potwierdzenia spełniania parametrów kategorii 7.

W celu rozróżnienia systemów należy zastosować różne kolory kabli. Poniżej przedstawiono sugerowany podział kolorystyczny:

- niebieskie – AP -przy gnieździe 5m patchcord, SKD, CCTV, SSWiN,
- czerwone - DECT – przy gnieździe 5m patchcord,
- zielone - Kolejkowy i przyzywowy,
- żółte – Integracja,
- szare – technologia, dodatkowe gniazda
- czarne – windy i BMS,
- pomarańczowe – inne

<u>Uniwersalny kabel optyczny 12 włóknowy jednomodowy, włókno OS2, G652D</u>

Okablowanie szkieletowe światłowodowe łączące punkty dystrybucyjne jest zrealizowane kablem światłowodowym jednomodowym (24 włóknowy kabel światłowodowy w osłonie trudnopalnej typu LSZH z włóknami jednomodowymi o rdzeniu 9/125µm). Aby zapewnić możliwość przesyłania nie tylko aktualnie stosowanych protokołów transmisyjnych, ale również długi okres działania sieci z odpowiednim zapasem pasma przenoszenia jako medium transmisyjne należy zastosować kabel światłowodowy jednomodowy 9/125µm z włóknami kategorii OS2 zalecanymi do transmisji od 10-100 Gigabitowych.

Włókna światłowodowe E9 OS2 z zerowym pikiem wodnym 652:

Zgodność z normami:

- IEC 60793-2-50 Kategoria B.1.3;
- ITU-T Zalecenie normą G.652.D i C, B, A
- IEEE 802.3 – 2002 incl. 802.3ae
- EN 50173-1:2007, kat. OS2; także wymagania OS1 są spełnione.
- ISO/IEC 11801:2002, kat. OS1
- SO/IEC 24702: 2006, kat. OS2; także wymagania OS1 są spełnione.

Tłumienność kabla z włóknami:

- 1310 - 1625 nm =<0,39 dB/km
- 1550 nm =<0,25 dB/km

Grupowy współczynnik refrakcji:

- 1310 nm 1,467
- 1550 nm 1,468
- 1625 nm 1,468

Wewnętrzno-zewnętrzny kabel wielotubowy, żelowany, optyczny 72 włóknowy jednomodowy, U-DQH, włókno OS2

Okablowanie szkieletowe światłowodowe do studni kablowej T/S/15 (gdzie będzie zamontowana mufa i przejście na kable 4E9) jest zrealizowane kablem światłowodowym (72 włóknowy kabel światłowodowy w osłonie trudnopalnej typu LSZH z włóknami jednomodowymi o rdzeniu 9/125µm 6x12 włókien w tubie o ø 2.5 mm). Aby zapewnić możliwość przesyłania nie tylko aktualnie stosowanych protokołów transmisyjnych, ale również długi okres działania sieci z odpowiednim zapasem pasma przenoszenia jako medium transmisyjne należy zastosować kabel światłowodowy jednomodowy 9/125µm z włóknami kategorii OS2 zalecanymi do transmisji od 10-100 Gigabitowych.

Włókna światłowodowe E9 OS2 z zerowym pikiem wodnym 652D:

Zgodność z normami

- EN 187 000
- ISO 11801 2ga edycja
- PN EN 50 173-1
- PN EN 60793-1-1
- PN EN 60793-2
- PN EN 60794-2
- PN EN 60794-3
- PN EN 41003;2001

Odporność ogniowa

- IEC 60332-1-2 Test pojedynczego pionowego kabla
- IEC 60754-1 Bez halogenu
- IEC 60754-2 Odporność kwasowa
- IEC 61034-2 Norma zadymienia spalania

Tłumienność kabla z włóknami

- 1310 - 1625 nm =<0,35 dB/km
- 1550 nm =<0,22 dB/km
- Wytrzymałość na rozciąganie (dynamiczne) 2100 N
- Uderzenie E4 10 Nm
- Średnica nominalna 11,3 mm
- Nominalna waga kabla 125kg/km
- Minimalny promień gięcia krótkotrwała 15xD, długotrwała 20xD

W celu łatwej identyfikacji wszystkie włókna światłowodowe mają być oznaczone przez producenta na całej długości różnymi kolorami, zaś osłona zewnętrzna powinna mieć kolor specjalny – dopuszcza się kolor czarny.

Należy przewidzieć zapasy kabla, przy szafie min. 10m oraz na stelażach zapasu w studni min. 15m.

Uniwersalny kabel optyczny 4 włóknowy E9 OS2

Okablowania dla gniazd końcowych (lokalizacja jak dla gniazd MATO, zgodnie z częścią rysunkową), jest zrealizowane kablem światłowodowym wielomodowym (4 włóknowy kabel światłowodowy w osłonie trudnopalnej typu LSZH z włóknami wielomodowymi o rdzeniu 50/125µm). Aby zapewnić możliwość przesyłania nie tylko aktualnie stosowanych protokołów transmisyjnych, ale również długi okres działania sieci z odpowiednim zapasem pasma

przenoszenia jako medium transmisyjne należy zastosować kabel światłowodowy wielomodowy 50/125µm z włóknami kategorii OM4 zalecanymi do transmisji 10/40/100-Gigabitowych.

Wymagania minimalne dla kabla światłowodowego OS2:

Zgodność z normami:

- IEC 60793-2-50 Kategoria B.1.3;
- ITU-T Zalecenie normą G.652.D i C, B, A
- IEEE 802.3 – 2002 incl. 802.3ae
- EN 50173-1:2007, kat. OS2; także wymagania OS1 są spełnione.
- ISO/IEC 11801:2002, kat. OS1
- SO/IEC 24702: 2006, kat. OS2; także wymagania OS1 są spełnione.
- IEC 60332-1-2, IEC 60754-1, IEC 60754-2, IEC 61034-2

Tłumienność kabla z włóknami

- 1310 - 1625 nm =<0,39 dB/km
- 1550 nm =<0,25 dB/km

Grupowy współczynnik refrakcji

- 1310 nm 1,467
- 1550 nm 1,468
- 1625 nm 1,468

Maksymalna siła ciągnienia 1000 N

Siła zrywająca 1500N

Uderzenie E7 15 Nm

Średnica nominalna 6,0 mm

Nominalna waga kabla 40kg/km

Minimalny promień gięcia krótkotrwała 60mm, długotrwała 100mm,

Temperatura pracy (°C): -40° do +60°

Osłona zewnętrzna: LSZH, 1.0mm niebieski odporna na UV, IEC 50290-2-27

Należy przewidzieć zapasy kabla, przy szafie min. 10m oraz na stelażach zapasu w studni min. 15m.

Przełącznica światłowodowa wysuwalna 1U 19”

Panel krosowy światłowodowy musi składać się z dwóch elementów: szuflady montażowej i płyty czołowej wymiennej 1U 24xSC simplex/ MTRJ/ E2000 oraz 1U 24xSCDuplex (LCQ) gwarantującej montaż adapterów LC.

Zastosowanie wymiennej płyty czołowej pozwala na migrację w przyszłości do różnych typów oraz ilości złącz optycznych. Producent musi dysponować w swojej ofercie płytami pozwalającymi na zakończenie od 12 włókien do 96 włókien na 1U. Kolor przełącznicy musi być zgodny i jednolity z całością systemu okablowania w części miedzianej.

Przełącznica musi posiadać dwie płaszczyzny wysuwania, 5 wejść kabla od tyłu, możliwość instalacji dławików kablowych oraz organizatorów przednich. Panel ma zapewnić zamontowanie 4 kaset światłowodowych.

Producent musi posiadać w swojej standardowej ofercie kompletne rozwiązania światłowodowe obejmujące cały tor transmisji tj. kabel krosowy o dowolnym interfejsie (w tym hybrydowe), adaptery i pigtaile światłowodowy (SC, LC, LCQUAD, ST, MTRJ, E2000, FC); tacki i osłonki spawów oraz elementy zaślepiające porty przełącznicy optycznej.

Adaptery LC/SC - parametry

- Obudowa – plastik
- Materiał rękawa centrującego - Fosforan brązu
- Kolor LC - beżowe lub turkusowe
- Maksymalna tłumienność - 0,20 dB
- Siła wcisku - 200-600 gram
- Wzrost tłumienności po 500 cyklach - 0,2 dB
- Temperatura pracy - od -40 do +80°C
- Stopień niepalności - UL94-V0

W adapterach światłowodowych (LC/SC) wymaga się stosowania zaślepek bezbarwnych – co umożliwia lokalizowanie toru światłem czerwonym bez konieczności demontażu zaślepki.

Pigtaile LC/PC OS2 (9/125 µm)

- Kable niskopalne LSZH.
- Zgodność z RoHS.
- Indywidualny numer seryjny na każdym produkcie.
- Maksymalna tolerancja długości wynosi + 6 - 0 cm.
- Polerowanie – UPC/APC – 8*
- Tłumienność – UPC/APC ≤ 0,3 dB
- Reflektancja – UPC ≤ 52 dB, APC ≤ 62 dB
- Rodzaj kabla - easy strip
- Średnica kabla - 900 µm
- Maksymalna siła naciągu przy instalacji – 6N
- Maksymalna siła naciągu po instalacji – 3N
- Minimalny promień zgięcia po instalacji – 30 mm
- Kolor kabla - żółty
- Kolor płaszcza – żółty

Kable krosowe HD światłowodowe SM G657B2 LC/UPC dupleks

System kabli krosowych HD jest dedykowany do punktów dystrybucyjnych i serwerowni gęstego upakowania (High Density). Kable muszą cechować się dużą elastycznością oraz posiadać specjalny klips pozwalający na wypięcie wtyku bez konieczności ingerowania w sąsiednie pola krosowe.

Minimalne wymagane parametry:

Tłumienność złącza (IEC 61300-3-4) IL: ≤10dB
Tłumienność złącza (IEC 61300-3-34) IL: ≤12dB
Tłumienność złącza UPC (IEC 61300-3-6) RL: ≤-55dB
Tłumienność włókna (dB/km): 1310nm: ≤0,38dB 1550nm: ≤0,23dB
Geometria feruli: Promień krzywizny (ROC dla UPC): 7-25mm,
Wysokość włókna (HEI): +/-50nm

Przesunięcie (OFFSET): 0-50µm
GRADE: B
Ilość cykli: 1000
typ odgiętki: 20mm

Wymagane normy:

IEC 61300-3-4
IEC 61300-3-34
25 Verizon FOC TPR-9409
GR-326 Core Issue 4
IEC, TIA/EIA JIS Spec

ROHS Compliant
UL 94V-0 Ruggedized
EN 187 000
IEC 60794-2
IEC 60794-2-10
ISO 11801 2nd edition
EN 50 173-1
LSHF-FR (FRNC): IEC 60332-1-2; IEC 60332-3-24; IEC 60754-2; IEC 61034, IEC 60794-1-2

Kolor złącza: SM niebieski RAL 5015
Kolor kabla: żółty RAL 1021
Materiał: Złącze: Plastik, stal nierdzewna, Ferula: Cyrkonia ZrO2
Rodzaj włókna: SM G657B2 (9/125µm)

Kable krosujące SM LC dupleks

- Kable niskopalne bezhalogenowe.
- Mechanicznie polerowane ceramiczne ferule.
- Zgodność z normą RoHS.
- Rodzaj kabla: SM G625.D
- Średnica rdzenia: 9µm
- Średnica kabla: 2 mm
- Maksymalna sił naciągu przy instalacji 400N
- Maksymalna sił naciągu w pracy 200N
- Minimalny promień zgięcia przy instalacji 30mm
- Minimalny promień zgięcia w pracy 45mm
- Kolor kabla: żółty

Aplikacja do integracji, monitorowania i zarządzania infrastrukturą serwerowni

W obiekcie należy zainstalować system pozwalający na uzyskanie informacji co do faktycznego stanu urządzeń i instalacji oraz podstawowych parametrów ich pracy. System ma umożliwiać szybką lokalizację alarmów, podstawowe logowanie danych czy też automatyczną reakcję na określone sygnały pochodzące z urządzeń. System w warstwie graficznej musi mieć możliwość jednoznacznego zaprezentowania dynamicznie zmieniających się informacji.

Podstawowe funkcje oprogramowania realizowane poprzez dynamicznie powiązane grafiki:

- Wizualizacja i zdalne sterowanie listwami zarządzalnymi oraz automatycznymi przełącznikami źródła zasilania (wszystkie funkcje, parametry, stany) zainstalowanymi w szafach serwerowych.
- Możliwość integracji z kontrolą dostępu zainstalowaną na obiekcie.
- Możliwość kontroli linii zasilających.
- Możliwość monitoringu wentylacji.
- Możliwość integracji z monitoringiem klimatyzacji.
- Możliwość monitorowania stanu UPS-ów.
- Możliwość monitorowania stanu agregatu prądotwórczego.
- Możliwość monitorowania rozdzielnic RE oraz jakości parametrów elektrycznych.
- Proste przemieszczanie pomiędzy widokami konkretnej instalacji, urządzeniami oraz innymi obiektami zintegrowanymi.
- Sygnały z systemu na bieżąco modyfikowane są grafiką, powodując zmianę koloru lub pulsowanie symboli, aktualizację wyświetlanej wartości, wyświetlanie komunikatu tekstowego oraz zmianę tekstu komunikatu lub symbolu.
- Obsługa alarmów zgłaszanych przez sterowniki i system (w tym alarmowe).
- Komunikaty wyświetlane wg priorytetów alarmów (pierwszy alarm pożarowy, drugi alarm bezpieczeństwa, itd.) i w kolejności chronologicznej.
- System musi zapewniać buforowanie wszystkich alarmów zgłaszanych jednocześnie.

- System musi umożliwiać rejestrację danych bieżących z monitorowanych instalacji i urządzeń w celu wykorzystania ich przy tworzeniu raportów - możliwość eksportu do programu MS Excel i innych baz danych.
- System uprawnień i zabezpieczeń musi umożliwiać dostęp tylko osobom upoważnionym. Każdy operator musi mieć przydzielone swoje dane identyfikacyjne i hasło.
- Możliowość pracy w trybie wieloekranowym oraz na urządzeniach mobilnych.
- Możliwość instalacji na maszynach wirtualnych.

Komunikacja i sposób transmisji:

- Transmisja pomiędzy urządzeniami jest realizowana na łączu Ethernet (łączność TCP / IP/UDP, IPX/SPX).
- Przeglądanie oraz sterowanie systemem z poziomu przeglądarki internetowej.
- Komunikacja pomiędzy aplikacjami za pośrednictwem sieci komputerowych XML, HTTP, HTML.
- Komunikacja z kartami wejść/wyjść włożonymi do komputera, na którym uruchomiony jest system - (np. kart AXIOM, MOXA, PCLab, Tedia, Advantech, Neovision, Elcom, National-Instruments, Biblioteki DLL, serwer OPC).
- Współpraca z bazami: dBase, EXCEL, Microsoft Access, Paradox, FoxPro, MS SQL Serwer, MySql, Oracle, itp.
- Obsługa SNMP, MODBUS, M-BUS, BACnet,
- Obsługa protokołów dostępnych dla sterowników PLC:Siemens,Simatic, SAIA, Mitsubishi, Allen-Bradley DF1, DF1 Koyo, Omron, Telemecanique, Modicon, ADAM, i inne.

Bezpieczeństwo:

- Administrator systemu musi mieć możliwość określenia, dla każdego operatora, odpowiedniego zakresu uprawnień pozwalającego dobrze zorganizować współpracę pomiędzy zarządzającym systemem, operatorami i innymi użytkownikami.
- Możliwość zablokowania wszystkich krytycznych klawiszy w Windows.
- Kontrola wykonywanej aplikacji: WatchDog programowy.
- Ochrona przed przepełnieniem dysku: struktura cykliczna trendów, alarmów i zdarzeń.
- Zabezpieczenie projektów w środowisku programowania poprzez hasło - ochrona "know how" użytkownika.

<u>Wymagania ogólne oraz dla instalatora</u>

Instalacja okablowania strukturalnego musi zostać wykonywana przez instalatora posiadającego ważne uprawnienia i certyfikat wydany przez producenta okablowania (Certyfikowany Instalator Systemu). Certyfikat instalatora, który posiada wykonawca instalacji musi być dokumentem terminowym wydawanym na okres maksymalnie dwóch lat. Po tym czasie instalator musi go przedłużyć na kolejny okres, uczestnicząc w szkoleniu realizowanym przez producenta. Zaleca się aby Wykonawca posiadał również ważny status Certyfikowanego Projektanta Systemu ze względu na procedurę gwarancyjną – projekt powykonawczy.

Uprawnienia Certyfikowanego Instalatora sytemu muszą obejmować wszystkie stopnie/poziomy kwalifikacji: Instalację, nadzór, serwis i kwalifikowanie do objęcia gwarancją niezawodności. Certyfikat musi być wystawiony przez Producenta systemu okablowania, nie dopuszcza się certyfikatu wystawionego przez dystrybutora, reselera, czy innego przedstawiciela nie będącego producentem. Certyfikat powinien być wystawiony w języku polskim, posiadać nazwę instalatora (firmy), nazwisko instalatora, zakres uprawnień oraz datę wystawienia certyfikatu.

Wymaga się, aby producent systemu okablowania strukturalnego spełniał wymagania jakościowe potwierdzone certyfikatem np. ISO 9001:2008 zarówno w zakresie działalności handlowej jak i produkcyjnej.

Wszystkie komponenty muszą charakteryzować się pełną zgodnością ze specyfikacją dla kategorii 6A (lub odpowiednio 7A dla punktów multimedialnych i połączeń pomiędzy szafami) (zgodnie z normą PN-EN 50173-1: 2011, oraz ISO 11801 2nd edition: 2002 Amd 2 2010). Zgodność parametrów modułów gniazd z obowiązującymi normami dla minimum kategorii 6A i odpowiednio 7A musi odpowiadać wymaganiom normy międzynarodowej, tj. ISO/IEC 11801:2011 oraz europejskiej tj. EN 50173-1 i fakt ten na etapie oferty musi zostać potwierdzony poprzez przedstawienie certyfikatów wydanych przez akredytowane (akredytacja typu AC), niezależne, notyfikowane laboratoria. Zgodność parametrów kabla instalacyjnego z obowiązującymi normami minimum kategorii 6A i odpowiednio 7A musi odpowiadać wymaganiom normy międzynarodowej, tj. ISO/IEC 11801:2011 i być na etapie oferty potwierdzona poprzez przedstawienie certyfikatów wydanych przez akredytowane (akredytacja typu AC), niezależne, notyfikowane laboratoria. Należy zapewnić również certyfikat z niezależnego laboratorium posiadającego akredytacje typu AC, potwierdzający zgodność łącza klasy EA i odpowiednio FA z normą ISO/IEC 11801 Ed.2.2 (2011-06) oraz EN 50173-1 (2011-09) w zakresie testu łącza 2 konektorowego Permanent Link.

Wszystkie komponenty muszą charakteryzować się pełną zgodnością ze specyfikacją dla kategorii 6A i odpowiednio kategorii 7A (zgodnie z normą ISO 11801 2nd edition: 2002 Amd 2.2 2011-06) oraz 8.2 zgodnie z dokumentem ISO-IECJTC1-SC25_N2238_25N2238_DTR_11801-99-1_IT pozwalające na uruchomieniu transmisji 25/40 GbE w przyszłości po spełnieniu wymagań standardu klasy II.

System składający się z komponentów kategorii 7A musi posiadać certyfikat niezależnego laboratorium posiadającego akredytacje typu AC, potwierdzający zgodność łącza klasy FA z normą ISO/IEC 11801 Ed.2.2 (2011-06) w zakresie testu łącza 2 konektorowego CHANNEL.

Wszystkie zastosowane kable teleinformatyczne miedziane i światłowodowe na stałe związane ze strukturą budynku muszą być zgodne z rozporządzenie PE i RUE nr 305/2011 oraz posiadać odpowiedni stopień klasyfikacji kabli pod względem pożarowym (Euroklasa) przewidziany dla danego typu obiektu zgodnie z klasyfikacją pożarową budynków . Potwierdzeniem powyższego jest przedstawienie przez wykonawcę odpowiedniej deklaracji własności użytkowych DoP a sam produkt (kabel) musi posiadać oznaczenie CE zgodnie z normami PN-EN 50575:2015-03/A1:2016-11

W celu optycznej identyfikacji wymaga się, aby wszystkie elementy okablowania (w szczególności: panele krosowe, gniazda, kable, kable krosowe, płyty czołowe gniazd, prowadnice kablowe) były oznaczone takim samym logiem systemu lub nazwą tego samego producenta. System okablowania strukturalnego musi obejmować kompletne rozwiązanie dla techniki miedzianej, światłowodowej, telekomunikacyjnej oraz szaf teleinformatycznych wraz z osprzętem. Wszystkie powyższe elementy muszą stanowić jeden i pełny system okablowania i pochodzić z jednorodnej oferty handlowej od jednego producenta. Elementy systemu okablowania powinny szczególnie być nastawione na uniwersalność, skalowalność, łatwość w montażu oraz prostotę i przejrzystość całości rozwiązań.

Zastosowanie rozwiązań jednego producenta dla sieci LAN musi być w takim stopniu w jakim pozwoli to na uzyskanie min. 25 letniej gwarancji systemowej oraz zapewni dopasowanie i kompatybilność elektromagnetyczną wszystkich elementów systemu okablowania strukturalnego. Wykonawca autoryzujący system okablowania strukturalnego musi posiadać uprawnienia do objęcia zainstalowanego systemu co najmniej 25-letnią systemową gwarancją niezawodności, udzielaną przez producenta okablowania.

<u>Wymagania szczegółowe</u>

- Wszystkie elementy pasywne (miedziane i światłowodowe, kable instalacyjne, panele, gniazda, kable krosowe), składające się na okablowanie strukturalne muszą być trwale oznaczone nazwą lub znakiem firmowym producenta i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu gwarancyjnego w/w producenta;

- maksymalna długość kabla instalacyjnego w łączu stałym (od punktu dystrybucyjnego do gniazda końcowego) nie może przekroczyć 90 metrów;
- projekt wymaga zastosowania kabla poziomego o wyższej niż opisana wydajności, celem zapewnienia Użytkownikowi zapasu transmisyjnego dla nowych usług i standardów transmisyjnych;
- Wszystkie komponenty powinny charakteryzować się pełną zgodnością ze specyfikacją dla minimum kategorii 6A, i odpowiednio 7A (zgodnie z normą PN-EN 50173-1: 2011, oraz ISO 11801 2nd edition: 2002 Amd 2 2010);
- Zgodność parametrów modułów gniazd z obowiązującymi normami minimum kategorii 6A i odpowiednio 7A musi odpowiadać wymaganiom Normy międzynarodowej, tj. ISO/IEC 11801:2011 oraz europejskiej tj. EN 50173-1 i być na etapie oferty potwierdzona poprzez przedstawienie certyfikatów wydanych przez akredytowane niezależne laboratoria (np. GHMT, 3P, Delta) potwierdzające zgodność systemu/komponentu z wymaganiami Normy międzynarodowej, tj. ISO/IEC 11801:2011. W przypadku dokumentów wystawionych przez inne niż wskazane akredytowane laboratoria certyfikujące, wymagane jest posiadanie przez tą instytucję akredytację typu AC (lub równoważnej) jednostki nadrzędnej w danym kraju (np. w Polsce jednostka nadrzędna to Polskie Centrum Akredytacji);
- Skrętka teleinformatyczna musi posiadać minimum jeden certyfikat niezależnego instytutu badawczego (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2((2011-06)), IEC 61156-5 Ed.2.1 (2012-12) dla potwierdzenia spełniania parametrów.
- Moduł RJ45 Keystone JACK musi posiadać minimum dwa certyfikaty dwóch niezależnych instytutów badawczych (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2((2011-06)), EN 50173-1((2011-11)), ANSI/TIA-568-C.2 ((2009-08))} dla potwierdzenia spełniania parametrów.
- Wydajność systemu okablowania (Permament Link) musi być potwierdzona certyfikatem przynajmniej jednego niezależnego akredytowanego laboratorium, np., GHMT, DELTA, itp.; certyfikaty muszą obejmować wszystkie aktualne normy okablowania normami {ISO/IEC 11801 ED.2.2((2011-06)), EN 50173-1((2011-09)), ANSI/TIA-568-C.2 ((2009-08))} .
- Wymóg posiadania powyższych certyfikatów jest uzasadniony z punktu widzenia gwarancji jakości i powtarzalności najwyższych parametrów komponentów i całego systemu.
- System okablowania strukturalnego powinien być objęty 25 letnią gwarancją systemową wystawianą przez producenta (gwarancja na szafy minimum 5 lat).
- Producent systemu okablowania musi posiadać certyfikat jakości EN ISO 9001:2008 w zakresie działalności handlowej i produkcyjnej.

Administracja i dokumentacja

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, tak od strony gniazda, jak i od strony szafy montażowej. Te same oznaczenia należy umieścić w sposób trwały na gniazdach sygnałowych w punktach przyłączeniowych użytkowników oraz na panelach.

Powykonawczo należy sporządzić dokumentację instalacji kablowej uwzględniając wszelkie, ewentualne zmiany w trasach kablowych i rzeczywiste rozmieszczenie punktów przyłączeniowych w pomieszczeniach. Do dokumentacji należy dołączyć raporty z pomiarów torów sygnałowych.

Odbiór i pomiary sieci

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest uzyskanie gwarancji systemowej producenta potwierdzającej weryfikację wszystkich zainstalowanych torów na zgodność parametrów z wymaganiami norm Klasy EA (oraz FA) wg obowiązujących norm.

W celu odbioru instalacji okablowania strukturalnego należy spełnić następujące warunki:

Wykonać komplet pomiarów – opis pomiarów części miedzianej i światłowodowej.

Wykonawstwo pomiarów powinno być zgodne z normą PN-EN 50346:2004/A1+A2:2009. Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą PN-EN 14763-3:2009/A1:2010. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

Należy użyć miernika dynamicznego (analizatora), który posiada wgrane oprogramowanie umożliwiające pomiar parametrów według aktualnie obowiązujących norm. Sprzęt pomiarowy musi posiadać aktualny certyfikat potwierdzający dokładność jego wskazań.

Analizator okablowania wykorzystany do pomiarów musi charakteryzować się przynajmniej IV klasą dokładności wg IEC 61935-1/Ed. 3 (proponowane urządzenia to np. Lantek 7G, FLUKE DTX 1800, PSIBER - WireXpert).

W przypadku sieci miedzianej pomiary należy wykonać w konfiguracji pomiarowej łącza stałego (ang. „Permanent Link") – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego

Pomiary należy skonfrontować z wydajnością klasy EA (oraz FA) specyfikowanej wg. ISO/IEC11801:2002/Am2:2010 lub EN50173-1:2011.

Pomiar każdego toru transmisyjnego poziomego (miedzianego) powinien zawierać:

- Attenuation – (Insertion Loss)
- NEXT - Near-End X-Talk
- ACR-N - Attenuation-to-Crosstalk Ratio NEXT;
- PS NEXT - PowerSum NEXT
- PS ACR-N - PowerSum ACR-N
- ACR-F - Attenuation-to-Crosstalk Ratio FEXT; dawniej ELFEXT – Equal Level FEXT
- PS ACR-F - PowerSum ACR-F; dawniej PS ELFEXT
- RL – Return Loss

Tłumienie światłowodowego toru transmisyjnego może być wyznaczone za pomocą miernika spadku mocy optycznej lub reflektometru.

Niezależnie od użytego sprzętu pomiarowego kompletny pomiar tłumienia każdego dupleksowego toru transmisyjnego powinien być przeprowadzony w dwie strony w dwóch oknach transmisyjnych dla dwóch włókien (chyba że typ złącza uniemożliwia taką procedurę):

- od punktu A do punktu B w oknie 1310nm i 1550nm (SM)
- od punktu B do punktu A w oknie 1310nm i 1550nm (SM)

Na raportach pomiarów powinna znaleźć się informacja opisująca wielkość marginesu (inaczej zapasu, tj. różnicy pomiędzy wymaganiem normy a pomiarem, zazwyczaj wyrażana w jednostkach odpowiednich dla każdej mierzonej wielkości).

Zastosować się do procedur certyfikacji producenta systemu okablowania strukturalnego.

<u>Wymagania gwarancyjne</u>

Wykonawca jest zobowiązany do dostarczenia aktualnej dokumentacji powykonawczej w postaci elektronicznej jak i w formie papierowej z pomiarami sieci logicznej i elektrycznej całość procedury jest opisana w dokumencie „Gwarancja Systemowa. Certyfikowany System Okablowania Strukturalnego ".

Po zakończeniu instalacji, Wykonawca wystąpi z wnioskiem do Producenta Okablowania o certyfikację instalacji kategorii 6A oraz 7A i po pozytywnie zakończonym audycie, dostarczy „Certyfikat" Użytkownikowi.

Gwarancja Systemowa na Certyfikowany System Okablowania Strukturalnego obejmuje:

A. Gwarancję produktową Wszystkie komponenty Certyfikowanego Systemu Okablowania Strukturalnego będą wolne od wad materiałowych i wad wykonania pod warunkiem ich prawidłowego montażu i eksploatacji.

B. Gwarancję wydajności Parametry łącza stałego lub kanału Certyfikowanego Systemu Okablowania Strukturalnego będą spełniać wymogi określone przez normy ISO/IEC 11801, EN 50173, PN-EN 50173-1, TIA/EIA 568A/B dla klasy wydajności, dla której łącze było zaprojektowane.

C. Gwarancję na pracę aplikacji Gwarancja nie jest ograniczona poprzez definiowane z góry poszczególnych protokołów transmisji możliwych do zastosowania przez Użytkownika. Certyfikowany System Okablowania Strukturalnego będzie umożliwiał transmisję sygnałów w oparciu o protokoły i aplikacje sieciowe zdefiniowane przez komitety normalizacyjne IEEE, ANSI, TIA/EIA oraz ATM Forum i zatwierdzonych do transmisji w oparciu o aktualne normy ISO/IEC 11801, EN 50173 , PN-EN 50173-1, TIA/EIA 568A/B.

Gwarancja Systemowa – procedura uzyskania gwarancji.

Pierwszym etapem procedury uzyskania Gwarancji Systemowej jest przesłanie do producenta okablowania wypełnionego Formularza Zgłoszeniowego przed rozpoczęciem instalacji.

Formularz Zgłoszeniowy zawiera podstawowe informacje dotyczące instalacji, Certyfikowanego Instalatora oraz terminów rozpoczęcia i zakończenia instalacji.

Producent zastrzega sobie możliwość kontroli instalacji podczas jej realizacji, jak również po jej zakończeniu.

Po wykonaniu instalacji do Producenta Systemu należy dostarczyć następujące dokumenty:

- Podpisany i ostemplowany komplet dokumentacji powykonawczej zawierającej schemat ideowy instalacji oraz projekty punktów dystrybucyjnych (szaf).
- Listę zainstalowanych komponentów wraz z kopiami faktur zakupowych.
- Wyniki pomiarów dynamicznych torów miedzianych łączy stałych lub kanałów (Permanent Link) oraz wyniki pomiarów tłumienia torów światłowodowych wykonanych według obowiązujących norm ISO/IEC 11801 lub EN 50173-1.

Pomiary światłowodowe muszą być wykonane w dwóch oknach, w dwóch kierunkach, należy wykonać przynajmniej pomiar tłumienności kanału.

Pomiary muszą być dostarczone w formacie elektronicznym miernika (.flt, .fcm, .dat, .mdb itp.).

Załączyć należy aktualne świadectwo kalibracji miernika użytego do wykonania pomiarów.

W przypadku stwierdzenia nieprawidłowości w wykonanej instalacji certyfikowany Instalator wykonuje niezbędne poprawki i zgłasza je do Producenta Systemu, po czym ustalany jest termin kontroli sieci (kontrola ta może być odpłatna).

Po potwierdzeniu właściwego wykonania instalacji przez Producenta Systemu wystawiona zostanie nieodpłatnie Gwarancja Systemowa na Certyfikowany System Okablowania Strukturalnego w postaci certyfikatu.

Wykonać dokumentację powykonawczą.

Dokumentacja powykonawcza ma zawierać:

- Raporty z pomiarów dynamicznych okablowania,
- Rzeczywiste trasy prowadzenia kabli transmisyjnych poziomych,
- Oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych,
- Lokalizację przebić przez ściany i podłogi.

Raporty pomiarowe wszystkich torów transmisyjnych należy zawrzeć w dokumentacji powykonawczej i przekazać inwestorowi przy odbiorze inwestycji. Drugą kopię pomiarów

(dokumentacji powykonawczej) należy przekazać producentowi okablowania w celu udzielenia inwestorowi (Użytkownikowi końcowemu) bezpłatnej gwarancji.

4.1.4 System Kontroli Dostępu

Założenia ogólne

Dla potrzeb Szpitala zaprojektowano w wybranych grupach pomieszczeń wykonanie instalacji systemu kontroli dostępu (SKD).

Ma on objąć swoim zasięgiem m.in. przejścia w ciągach komunikacyjnych, pomieszczenia techniczne (np. serwerownię), windy. Przejścia objęte KD pokazano na rysunkach oraz schemacie blokowym.

Jako sposób identyfikacji osób system będzie wykorzystywał karty zbliżeniowe. Zaprojektowany system pozwala na sieciową pracę urządzeń (zarządzanie, konfiguracja i rejestracja zdarzeń) oraz na sukcesywną rozbudowę. Poprawna identyfikacja osoby pozwala na otwarcie drzwi automatycznych lub zwolnienie elektrozaczepu/zamka drzwi. Z uwagi na uniwersalność i izolację galwaniczną obwodów elektrycznych instalacji współpracujących z instalacją kontroli przejścia do przekazania sygnału identyfikacji wykorzystuje się bezpotencjałowe styki (NO/NC) przekaźników wyjściowych kontrolerów. Jako element wykonawczy do blokowania drzwi nieautomatycznych zaproponowano elektrozaczepy rewersyjne NO z mikroprzełącznikiem (informacja o stanie otwarcia drzwi), w wybranych lokalizacjach zastosowano zamki rewersyjne (szczegóły wg zestawień architektury). Wejście do pomieszczenia jest możliwe po poprawnej identyfikacji (od strony wejścia drzwi wyposażone w pochwyt), wyjście po poprawnej identyfikacji (przejścia objęte dwustronną kontrolą) lub naciśnięciu klamki (przejścia objęte jednostronną kontrolą).

Wszystkie drzwi nieautomatyczne objęte kontrolą przejścia winny posiadać samozamykacze.

Zaprojektowane sterowniki drzwiowe kontroli przejścia zasilane są z zasilaczy 24V DC z funkcją podtrzymania pracy przy zaniku napięcia w sieci 230V AC. Elementy blokujące: elektrozaczepy i zamki zasilane są z zasilaczy 12VDC także z podtrzymaniem napięcia. W obwód zasilania elementów blokujących włączony jest styk elementu kontrolno-sterującego z instalacji sygnalizacji pożarowej (lub przekaźnika pomocniczego) oraz instalacji interkomowej. Rozwiązanie to pozwala na natychmiastowe zwolnienie blokad drzwi w przypadku wykrycia pożaru przez system sygnalizacji pożarowej lub w przypadku wyłączenia zasilania budynku wyłącznikiem przeciwpożarowym. Pozwala także na wysterowanie otwarcia przejścia z instalacji interkomowej. Drzwi zabezpieczono przed przypadkowym otwarciem w wyniku zaniku napięcia elementami blokującymi zasilanymi z zasilacza 12VDC z podtrzymaniem napięcia. Zwolnienie drzwi następuje poprzez wyłączenie zasilania sygnałem z instalacji sygnalizacji pożarowej lub lokalnie poprzez przyciśnięcie przycisku alarmowego otwarcia drzwi (po zbiciu szybki). Zwolnienie danego przejścia musi odbywać się poprzez fizyczne zdjęcie napięcia z elementu ryglującego.

Kontrolę dwustronną realizowaną w oparciu o dwa czytniki kontroli dostępu, zlokalizowane na wejściu i wyjściu do strefy należy zainstalować min. w ramach klatek schodowych przy szatniach Pozostałe przejścia zlokalizowane w pomieszczeniach należy objąć kontrolą jednostronną monitorowaną. W przypadku przejścia jednostronnego, na wejściu do strefy musi zostać umieszczony czytnik kontroli dostępu, na wyjściu ze strefy musi być umieszczony przycisk wyjścia podłączony do kontrolera kontroli dostępu.

W drzwiach objętych systemem kontroli dostępu zostaną zainstalowane zamki elektromagnetyczne rewersyjne, elektrozaczepy lub elektrozwory, czytniki zbliżeniowe umożliwiające otwarcie drzwi za pomocą kart zbliżeniowych oraz przyciski wyjścia ewakuacyjnego umożliwiające awaryjne otwarcie drzwi w przypadku ewakuacji. W ościeżnicach drzwi zainstalowane zostaną kontaktrony do sygnalizacji i rejestracji otwarcia drzwi.

System KD jest obsługiwany z poziomu serwera SMS, na którym zostaną zainstalowane odpowiednie licencje umożliwiające działanie systemu. Miminimalne parametry serwera podano w części dotyczącej SMS.

W projekcie przewidziano monitoring wejść do pomieszczeń technicznych. Każde skrzydło drzwi należy wyposażyć w kontaktron i podpiąć go do wejść sterowników drzwiowych SKD.

Topologia systemu

Aby zabezpieczyć bezproblemowe działanie zaprojektowanego systemu, na wypadek braku komunikacji lub uszkodzenia serwera, inteligencja musi zostać rozproszona do poziomu lokalnych sterowników. Przewodowy system posiada możliwość podłączenia czytników w oparciu o architekturę- gwiazdy, serwer komunikuje się z dedykowanymi sterownikami sieciowymi przez sieć TCP/IP. Każdy ze sterowników sieciowych obsługuje do 32 kontrolerów drzwiowych, a każdy kontroler drzwiowy co najmniej 2 czytniki. Sumarycznie w architekturze gwiazdy, sterownik obsługuje co najmniej 64 czytniki.

Okablowanie

Sterownik sieciowy jest podłączony do przełącznika sieci systemów bezpieczeństwa poprzez okablowanie LAN systemu bezpieczeństwa – kabel kat 6A. Połączenie pomiędzy sterownikiem sieciowym a kontrolerami drzwiowymi działa na zasadzie magistrali - realizowane jest kablem UTP kat. 6. Dla podłączenia czytnika, kontaktronu oraz przycisku wyjścia do kontrolera drzwiowego wymagany jest kabel UTP kat. 6 dla każdego z elementów.

Kontroler sieciowy, kontroler drzwiowy oraz elektrozaczep wymagają doprowadzenia zasilania kablem typu OMY 3x1,5 mm.

Sterownik sieciowy

Elementami wykonawczymi systemu kontroli dostępu będą inteligentne sterowniki sieciowe. Sterownik będzie komunikować się z serwerem za pomocą standardu TCP/IP i będzie pracował w środowisku LINUX. W przypadku zerwania łączności kontrolera sieciowego z serwerem, będzie on nadal zarządzać elementami do niego podłączonymi. Po ponownym podłączeniu go do serwera musi nastąpić automatyczna, wzajemna synchronizacja. Sterownik sieciowy będzie zarządzał max 4 kontrolerami sieciowymi, do których będzie doprowadzona magistrala RS485, na której będzie znajdować się do 8 kontrolerów drzwiowych. Każdy kontroler sieciowy podłączony do sterownika sieciowego ma za zadanie obsłużyć nie więcej niż 16 czytników.

Sterowniki sieciowe zostaną doposażone w akumulator 7Ah pozwalające na podtrzymanie zasilania przez 12 godzin.

Poniżej przykładowe obliczanie dla maksymalnego wyposażenia sterownika w 4 magistrale:

Element	**Pobór [W]**	**Ilość**	**Pobór razem [W]**	**Całkowity pobór prądu [A]**	**Podtrzymanie 12h [Ah]**	**Podtrzymanie 12h [Ah]*1,25 (współczynnik bezpieczeństwa)**
Sterownik sieciowy	2,5	1	2,5			
Kontroler drzwiowy (1 magistrala)	0,48	4	1,92			
SUMA			4,42	0,37	4,42	**5,525**

Kontroler sieciowy

Kluczowym urządzeniem wykonawczym systemu kontroli dostępu jest kontroler drzwiowy odpowiedzialny za zabezpieczenie dwóch przejść pojedynczych lub jednego przejścia podwójnego.

W zależności od charakterystyki poszczególnych obiektów, kontroler drzwiowy będzie działał zarówno w topologii gwiazdy, jak i magistrali w zależności od stosowanego typu sterownika sieciowego. Projektowane rozwiązanie oparto o topologię magistrali.

Projektowany kontroler drzwiowy musi obsługiwać do dwóch czytników kontroli dostępu i komunikować się z nimi za pomocą protokołów Clock/Data / Wiegand. W zależności od typu architektury kontroler musi oferować 8 wejść i 4 wyjścia (gwiazda) lub 8 wejść i 8 wyjść (magistrala) do podłączenia elementów wykonawczych (kontaktronów, zwór, elektrozaczepów, przycisków wyjścia, czy przycisków ewakuacyjnych).

Kontroler będzie miał możliwość dodatkowo podłączenie i ciągły pomiar mierników parametrów środowiskowych – temperatury i wilgotności. Jeden kontroler musi umożliwiać podłączenie co najmniej 4 mierników na dedykowanej magistrali.

Kontroler drzwiowy musi być wyposażony w specjalny system monitorowania stanu kontrolera (autotest), umożliwiający ciągły pomiar m.in.: wewnętrznej temperatury, parametrów zasilania kontrolera i czytników oraz stanu komunikacji z czytnikami. Stan urządzenia powinien być sygnalizowany wielokolorową diodą oraz być przesyłany do oprogramowania zarządzającego w czasie rzeczywistym. Dodatkowo kontroler drzwiowy musi być wyposażony w buzzer, włączany zdalnie informujący o miejscu instalacji kontrolera.

Kontrolery drzwiowe doposażone w akumulator 7Ah pozwalające na podtrzymanie zasilania przez 12 godzin.

Poniżej przykładowe obliczenia:

Element	Pobór [W]	Ilość	Pobór razem [W]	Całkowity pobór prądu przy zasilaniu 12V [A]	Podtrzymanie 12h [Ah]	Podtrzymanie 12h [Ah]*1,25 (współczynnik bezpieczeństwa)
Kontroler drzwiowy	0,48	1	0,48			
Czytnik	0,7	2	1,4			
Elektrozaczep	3	1	3			
SUMA			4,88	0,41	4,88	**6,1**

Czytniki

W ramach infrastruktury systemu kontroli dostępu na obiekcie zostaną zainstalowane czytniki oraz karty w standardzie zbliżeniowym MifareDESFire odczytujące numer seryjny karty kontroli dostępu.

Dodatkowo na obiekcie zostaną zainstalowane czytniki odczytujący dodatkowo kod QR z biletów systemu kolejkowego oraz czytniki przeznaczone pod system RCP. Czytniki systemu RCP informujące o początku/ końcu pracy oraz wyjściach służbowych/prywatnych zostaną umieszczone w specjalnej obudowie z dokładnym rozróżnieniem jaką funkcję spełnia. Informacje będą wysyłane do systemu kadrowo płacowego w formie pliku xml. System będzie wyposażony w czytniki o takich samych parametrach jak czytniki systemu KD. System RCP będzie obsługiwany przez te same karty co system KD.

Czytniki będą produkowane przez tego samego producenta, który produkuje pozostałe elementy systemu kontroli dostępu (sterowniki, kontrolery drzwiowe, oprogramowanie). Gwarantuje to niezawodną pracę całego systemu.

Wyjątkiem jest czytnik odczytujący dodatkowo kod QR z biletów systemu kolejkowego.

Czytniki kontroli dostępu muszą mieć możliwość odczytu szerokiego spektrum technologii zbliżeniowych: Mifare 1K, Mifare 4K, MifareDESFire, MifareDESFire EV1. Dodatkowo muszą mieć możliwość komunikacji za pomocą różnych protokołów transmisyjnych: Wiegand, Clock / Data, RS-485. Wykorzystując technologię zbliżeniową MifareDESFire, czytniki muszą umożliwiać szyfrowanie od karty przez czytnik do kontrolera (End-to-End security) z wykorzystaniem protokołu AES-256. Dzięki temu nie jest możliwe przechwycenie danych transmisyjnych przez osoby trzecie.

Czytnik będą wyposażone w czujnik ruchu, który wzbudzi czytnik w stan odczytu karty tylko w momencie, gdy zbliżona zostanie do niego karta dostępowa. Dzięki temu możliwa jest znaczna redukcja zużycia energii. Czytnik będzie wyposażony w wielotonowy brzęczyk, który realizuje sygnalizację dźwiękową o różnych tonach w zależności od rodzaju reakcji czytnika (przejście otwarte, brak dostępu itp.). Jest to funkcjonalność szczególnie pomocna dla osób niewidomych. Wszystkie elementy elektroniczne znajdujące się wewnątrz obudowy czytnika powinny być zalewane żywicą epoksydową. Dzięki temu czytniki są odporne na niekorzystne warunki atmosferyczne. Czytniki muszą posiadać normę szczelności min. IP64.

System KD musi umożliwiać podłączenie szerokiego zakresu czytników kontroli dostępu. System kontroli dostępu musi mieć możliwość komunikacji z czytnikiem za pomocą protokołów szeregowych. System musi obsługiwać czytniki karty z osobnymi modułami Mifare DESFire ISO/IEC 14443 Type A.

Realizowane funkcje

Głównym zadaniem systemu kontroli dostępu jest zarządzanie dostępem do poszczególnych obszarów zlokalizowanych na terenie obiektu. Zaprojektowany system KD ma uniemożliwić wejście do konkretnej strefy KD osobom nieuprawnionym. System KD musi mieć możliwość definiowania harmonogramu terminowego dostępu do stref KD dla poszczególnych użytkowników lub grup użytkowników. Harmonogramy muszą mieć możliwość działania w pętli. Dodatkowo system KD musi umożliwiać definiowanie harmonogramów czasowych definiujących prawa dostępu w konkretnym dniu z dokładnością do jednej minuty.

System kontroli dostępu musi również umożliwiać śledzenie i lokalizowanie osób przemieszczających się w obrębie chronionych stref. System musi mieć możliwość generowania raportów na temat ilość osób znajdujących się w poszczególnych strefach, dzięki czemu możliwa jest np. optymalizacja akcji ewakuacyjnej. Dodatkowo system powinien umożliwiać definiowanie na klawiaturze operatora klawisza szybkiego wyboru, który automatycznie generuje raport zawierający listy osób przebywających na obiekcie, z podziałem na strefy KD. System KD musi mieć możliwość sprawdzenia gdzie poszczególni użytkownicy znajdują się w czasie rzeczywistym i gdzie znajdowali się w wybranym momencie w przeszłości. Dzięki temu możliwa jest weryfikacja, np. jakie osoby znajdowały się w pomieszczeniu w momencie kradzieży mienia. Dodatkowo w oparciu o dane odnośnie liczby osób przebywających w poszczególnych pomieszczeniach, system umożliwia rozpoczęcie automatycznych procedur, np. wyłączenie zasilania i zazbrojenie strefy SSWiN po opuszczeniu przez wszystkich użytkowników danej strefy.

Zaprojektowany system będzie w pełni skalowalny i wymaga się aby obsługiwał w ramach jednego serwera zarządzającego, co najmniej 100 000 aktywnych kart (użytkowników) i nie mniej niż 1536 grup kart. System KD musi dodatkowo wspierać co najmniej 2000 czytników oraz kontrolerów kontroli dostępu w ramach jednego serwera. Musi być możliwość podłączenia na wejścia kontrolerów co najmniej 8192 elementów zewnętrznych (przyciski wyjścia, alarmowe, kontaktrony itp.). Dzięki temu możliwa będzie bezproblemowa rozbudowa systemu KD w przyszłości.

System KD musi mieć również możliwość obsługi gości poprzez dodanie przez użytkowników do systemu informacji o przyjeździe gościa, którą otrzymuje operator systemu. Dodatkowo musi być możliwość przypisania do danej osoby numeru rejestracyjnego samochodu. Operator musi mieć możliwość przygotowania dla gościa specjalnej, spersonalizowanej karty z tymczasowymi prawami dostępu do wyznaczonych pomieszczeń, gdzie mają miejsce spotkania.

System KD musi zabezpieczać przed niewłaściwym użyciem karty przez użytkowników oraz sygnalizować sytuacje alarmowe. W tym celu musi realizować poniższe funkcjonalności:

- Funkcję globalnego Anti-Pass Back z podziałem na strefy (wsparcie dla Anti-Pass Back globalnie, punktowo, czasowo, rewersyjnie).
- Funkcję śluzowości obsługującą do 16 wejść.
- Funkcję unieważniania kart zbyt długo nieużywanych zabezpieczająca przed użyciem zagubionej karty, np. karta nie użyta na jednym z czytników w ciągu 24 godzin traci swoje prawa dostępowe.
- Funkcję kwarantanny, która zabrania użytkownikom wejście do określonych stref, jeżeli wcześniej znajdowali się w innej, ściśle zdefiniowanej strefie.
- Funkcję nadawania praw użytkownikom, w momencie gdy znajdowali się w innej strefie, np. karta jest ważna na terenie magazynu, tylko w momencie gdy wcześniej została użyta w portierni.
- Element ryglujący musi dokonywać zaryglowania przejścia niezwłocznie po zamknięciu drzwi przez osobę wchodzącą do pomieszczenia (element ryglujący nie czeka, aż skończy się czas odryglowania ustawiony w systemie).
- Funkcję wzbudzenia alarmu w momencie gdy drzwi na zbyt długi czas pozostają otwarte.
- Funkcję wejścia pod przymusem polegającą na zapisaniu dla danego użytkownika dwóch haseł pin. W momencie gdy dany użytkownik wchodzi pod przymusem do strefy, przykłada kartę i wpisuje hasło dedykowane dla wejścia pod przymusem. Uzyskuje on dostęp do danej strefy, jednocześnie operator zostaje powiadomiony o fakcie wejścia pod przymusem.
- Funkcję rozbudowanych alarmów kontroli dostępu, w których alarm jest wzbudzony w momencie gdy karta zostaje uznana jako skradziona, lub użytkownik przyłoży do kartę do czytnika do którego nie ma uprawnień.

System musi umożliwiać zmianę stanu przejścia. W systemie muszą być wyróżnione następujące tryby pracy przejścia kontroli dostępu:

- Otwarte – element ryglujący jest nieaktywny;
- Normalny – kontrola dostępu zgodna z harmonogramem i uprawnieniami użytkowników;
- Zablokowany – element ryglujący zaryglowany, czytnik zablokowany i nie odczytuje kart dostępowych;
- Z potwierdzeniem – W momencie gdy użytkownik przykłada kartę dostępową operatorowi prezentowane jest okno w którym widoczne jest zdjęcie właściciela karty z bazy systemowej oraz obraz z kamery (w przypadku integracji systemu CCTV). Operator potwierdza czy dana osoba może wejść do danej strefy kontroli dostępu.

Uprawniony operator musi mieć możliwość zmiany w czasie rzeczywistym trybu pracy danego czytnika kontroli dostępu z poziomu mapy synoptycznej. System musi dodatkowo mieć możliwość zmiany trybu pracy czytnika w zależności od stanu systemu (stan systemu normalny, alarmowy itp.).

Wszystkie zdarzenia mające miejsce w systemie są zapisywane w bazie danych systemu. System umożliwia pełne raportowanie i archiwizację danych. System musi mieć wbudowane predefiniowane raporty, m.in:

- Raport obecności dla danego użytkownika i dla danego obszaru;
- Raport praw dostępu dla użytkownika i czytnika;
- Raport ścieżki użycia karty na obiekcie;
- Raport stanu sterowników i podłączonych do nich urządzeń;
- Raport kart według grup kart;
- Raport kart według typu kodowania.

Dodatkowo w systemie musi być dostępny generator raportów, który umożliwia generowanie dowolnych raportów według wymogów operatora.

Projektowany system kontroli dostępu jest również dostosowany do obsługi przez osoby niepełnosprawne, przez wydłużenie czasu zwolnienia elementu ryglującego w momencie przyłożenia karty przez osobę niepełnosprawną. Dzięki temu osoba niepełnosprawna może bez problemów przemieszczać się po obiekcie.

4.1.5 System Sygnalizacji Włamania i Napadu (SSWiN)

Ogólne założenia

Projektuje się instalację sygnalizacji włamania obejmującą pomieszczenia na kondygnacjach B01 oraz P05. Instalacje te mają za zadanie ochronę wybranych pomieszczeń przed włamaniem lub wejściem niepożądanych osób oraz zapewnić bezpieczeństwo obsługi w przypadku napadu. Ochrona pomieszczeń przed włamaniem będzie realizowana poprzez zastosowanie detektorów:

- kontaktronów magnetycznych w oknach i drzwiach
- czujek ruchu dualnych pasywnych podczerwieni i mikrofalowych
- czujek akustycznych zbicia szkła

Ochrona przed napadem będzie realizowana w oparciu o:

- ręczne przyciski napadowe przewodowe (bezprzewodowe)

Odpowiednie rozmieszczenie czujek zapewni wytworzenie stref ochronnych, które obejmują pomieszczenia określone przez Inwestora. Rozmieszczenie elementów sytemu pokazano na podkładach budowlanych.

Zarządzanie systemem

Zarządzanie systemem SWiN bedzie możliwe z poziomu:

- Mapy synoptycznej – zazbrajanie i rozbrajanie poszczególnych stref SSWiN oraz wizualizacja stanów poszczególnych stref i elementów detekcyjnych nawet w momencie gdy strefa nie jest zazbrojona.
- Czytnika kontroli dostępu – automatyczne zazbrajanie i rozbrajanie poszczególnych stref SSWiN po przyłożeniu uprawnionej karty dostępowej lub w momencie gdy wszystkie osoby wyjdą z pomieszczenia (realizowane w oparciu o czytniki kontroli dostępu). Wizualizacja stanu strefy SSWiN na diodzie czytnika kontroli dostępu.
- Manipulatora SSWiN – zazbrajanie i rozbrajanie po wpisaniu kodu autoryzacyjnego. Wizualizacja stanów poszczególnych stref. Konfiguracja systemu zgodnie z uprawnieniami.
- Aplikacji mobilnej – zazbrajanie i rozbrajanie po wpisaniu kodu autoryzacyjnego. Wizualizacja stanów poszczególnych stref. Konfiguracja systemu zgodnie z uprawnieniami.

Topologia systemu

Jako centralny punkt systemu projektuje się centralę alarmową. Centrala alarmowa będzie miała wbudowany na płycie głównej centrali interfejs TCP/IP. Centrala musi być w pełni skalowalna i domyślnie oferować jedną magistralę transmisyjną. W obrębie samej centrali musi być wbudowany moduł obsługi 16 linii dozorowych, 1 wyjścia przekaźnikowego i 4 wyjść OC. Pozostałe linie dozorowe powinny być podłączane do ekspanderów linii dozorowych, dołączonych do magistrali (maksymalnie 120 linii dozorowych na magistralę). Dodatkowo centrala musi umożliwiać rozbudową o jedną lub cztery dodatkowe magistrale transmisyjne za pomocą dedykowanej płyty rozszerzeń magistral (instalowanej bezpośrednio na płycie głównej centrali). Pojedyncza centrala musi obsłużyć maksymalnie do 616 linii dozorowych.

Zaprojektowana centrala będzie obsługiwała dwie magistrale. Pierwsza będzie podłączona do magistrali transmisyjnej w która domyślnie jest wyposażona centrala, Druga magistrala zostanie podłączona do płyty rozszerzeń magistrali.

Centrala musi mieć możliwość podłączenia do każdej magistrali co najmniej 15 ekspanderów przewodowych lub bezprzewodowych, każdy wyposażony w 8 linii dozorowych. Do każdej centrali musi być możliwość podłączenia maksymalnie 40 klawiatur kodowych (manipulatorów) do zarządzania strefami.

Centrala SSWiN musi być zgodna z wymogami norm PN-EN 50131 dla systemu stopnia 3. Zgodność musi być potwierdzona certyfikatem akredytowanej europejskiej jednostki certyfikacyjnej oraz polskiego Zakładu certyfikacyjnego TECHOM.

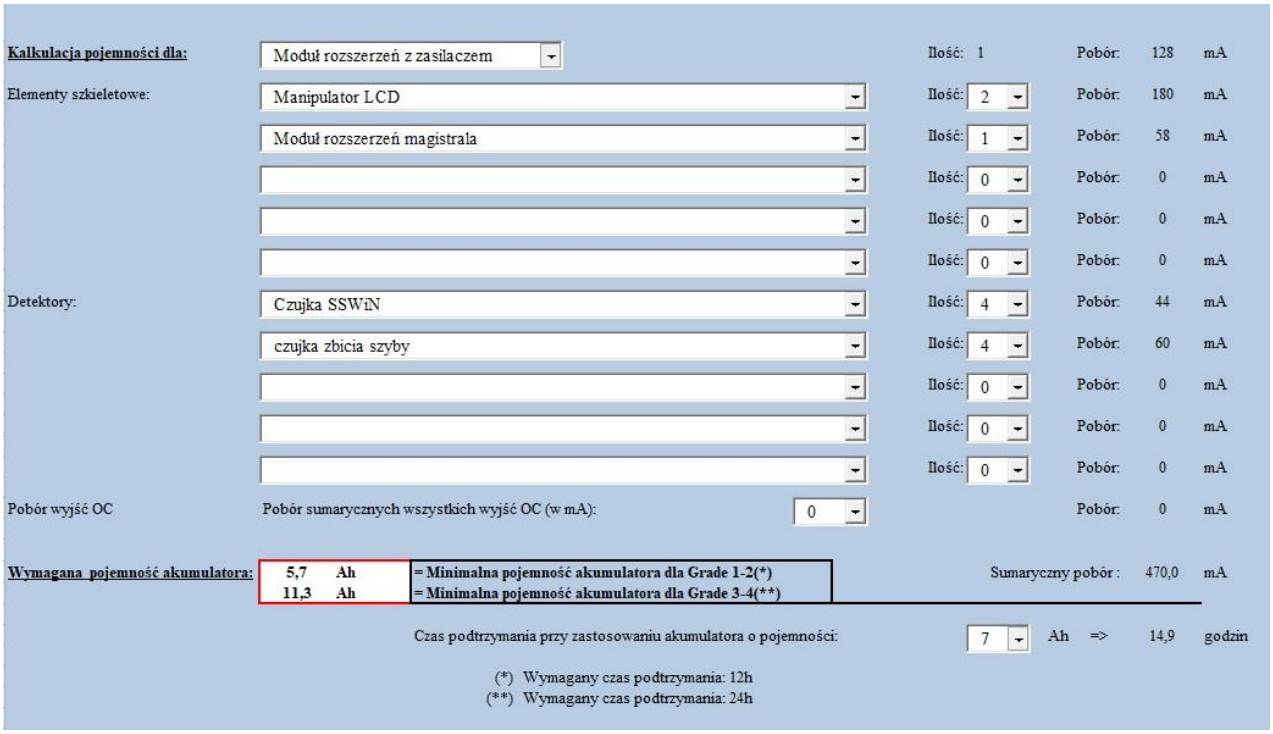
Centrala zostanie doposażona w akumulator 7,3Ah pozwalający na podtrzymanie zasilania systemu przez min 24 godziny. Poniżej przykładowe wyliczenie:

Kalkulacja pojemności dla:	Centrala SSWiN XL		Ilość: 1	Pobór:	100	mA
Elementy szkieletowe:	Manipulator LCD		Ilość: 2	Pobór:	180	mA
	Dialer PSTN XL (moduł instalowany na płycie centrali)		Ilość: 1	Pobór:	10	mA
			Ilość: 0	Pobór:	0	mA
			Ilość: 0	Pobór:	0	mA
			Ilość: 0	Pobór:	0	mA
Detektory:	Czujka SSWiN		Ilość: 1	Pobór:	11	mA
			Ilość: 1	Pobór:	0	mA
			Ilość: 0	Pobór:	0	mA
			Ilość: 0	Pobór:	0	mA
			Ilość: 0	Pobór:	0	mA
Pobór wyjść OC	Pobór sumarycznych wszystkich wyjść OC (w mA):	0		Pobór:	0	mA
Wymagana pojemność akumulatora:	**3,7 Ah**	**= Minimalna pojemność akumulatora dla Grade 1-2(*)**		Sumaryczny pobór :	301,0	mA
	7,3 Ah	**= Minimalna pojemność akumulatora dla Grade 3-4(**)**				
	Czas podtrzymania przy zastosowaniu akumulatora o pojemności:		7 Ah	=>	23,3	godzin

(*) Wymagany czas podtrzymania: 12h
(**) Wymagany czas podtrzymania: 24h

Ekspandery z zasilaczem zostaną doposażone o akumulatory 12 Ah pozwalający na podtrzymanie zasilania systemu przez min 24 godzin.

Poniżej przykładowe wyliczenie:



Okablowanie

Centrala SSWiN zostanie podłączona do przełącznika sieci systemów bezpieczeństwa poprzez okablowanie LAN systemu bezpieczeństwa – kabel SFTP cat6A. Polaczenie pomiędzy centralą a ekspanderami jest połączeniem typu magistrala - realizowane jest kablem FTP cat. 6. Dla podłączenia detektorów, kontaktronów, przycisków napadowych do ekspandera lub centrali zalecany jest kabel typu JY(St)Y 2x2x0.6.

Centrala SSWiN oraz ekspandery z zasilaczami wymagają doprowadzenia zasilania kablem typu OMY 3x1,5 mm.

System SSWiN musi dawać możliwość rozbudowy systemu w przyszłości o kolejne centrale SSWiN oraz sieciowanie ich za pomocą interfejsu SMS.

Parametry głównych urządzeń

Wymagane dodatkowe parametry centrali:

- Komunikacja:
  - dialer IP zintegrowany na płycie głównej centrali,
  - możliwość podłączenia dialera PSTN
  - możliwość podłączenia dialera GPRS
- Czujnik antysabotażowy
- Klasa (Grade): 3
- Kody użytkownika: 500 (9 poziomów)

Poniżej przedstawiono wymagania odnośnie kluczowych parametrów ekspanderów linii i manipulatora kontrolnego:

Ekspander 8 linii z zasilaczem:

- Moduł rozszerzenia centrali alarmowej umożliwiający podłączenie detektorów.
- Wejścia: 8x NO, NC, EOL, DEOL; 3x antysabotaż
- 9 wyjść:
  - 2 przekaźnikowe,
  - 6 OC (max 100mA),

  - 1 głośnikowe (8 om).
- Komunikacja: RS485.

Manipulator kontrolny:

- Wymiary: 164 x 124 x 28 mm
- Napięcie: 12 VDC
- Temp./ Wilgotność: 0°C do +50°C, do 90% bez kondensacji
- Komunikacja: RS485
- Inne cechy: buczek, wyświetlacz LCD 2x16 znaków
- 8 diod LED sygnalizujących stan systemu

4.1.6 System Wideointerkomowy

Ogólne założenia

Aby zapewnić szybką i sprawną komunikację przy wejściach na oddziały zaprojektowano system interkomowy. System oparty jest o fizyczny serwer interkomowy z zainstalowanym oprogramowaniem oraz licencjami do obsługi systemu oraz stacji interkomowych IP oraz stacji cyfrowych.

Stacje interkomowe

Stacje interkomowe zostaną zlokalizowane przy wejściach na dane oddziały oraz w dyżurkach, a także w pięciu salach operacyjnych znajdujących się na kondygnacji P02.

Przy wejściach na oddziały projektuje się stacje naścienne z jednym przyciskiem oraz kamerą. Stacje będą komunikowały się z dyżurką danego oddziału – na wyświetlaczu interkomu będzie wyświetlany obraz z kamery interkomu.

Interkomy znajdujące się w pom. pielęgniarki dyżurnej będą wyposażone w interkom z wyświetlaczem ISP oraz słuchawką. Na wyświetlaczu interkomu będzie można zarówno stworzyć listę najczęściej wybieranych numerów jak i wywołać połączenie poprzez wybranie odpowiedniego numeru.

Pielęgniarka będzie miała także możliwość wdzwonić się na telefony VoIP zainstalowanie w szpitalu.

Dodatkową funkcja będzie także możliwość otwarcia drzwi przy których znajduje się stacja wywoławcza interkomu poprzez przyciśnięcie dowolnie skonfigurowanego przycisku na wyświetlaczu stacji.

Naciśnięcie danego przycisku przypisanego do danego interkomu spowoduje zwolnienie KD na danych drzwiach.

Interkomy przy wejściach na oddziały oraz na stanowiskach pielęgniarskich są interkomami IP i wymagają wpięcia do lokalnej sieci LAN a także zasilenia poprzez dedykowany zasilacz lub z przełacznika z PoE.

Interkomy znajdujące się na salach operacyjnych na kondygnacji P02 są interkomami cyfrowymi „czystymi" z pełną klawiaturą oraz wyświetlaczem LCD. Ze względu na wymaganą sterylność pomieszczenia oraz przeprowadzany w salach proces dekontaminacji interkomy musza posiadać atest higieniczny Państwowego Zakładu Higieny. Dodatkowo stacje interkomowe powinny posiadać potwierdzenie spełniania wymagań Kompatybilności Elektromagnetycznej opisanych normami, min :EN 55022:2006+A1:2007, EN 55024:1998+A1:2001+A2:2003, EN61000-6-2:2007, EN61000-6-3:2007.
Instalacja interkomu ma umożliwić komunikację głosową Zespołu Zabiegowego z dowolnym interkomem na obiekcie oraz z dowolnym telefonem. Lokalizację instalacji interkomu wskaże Zamawiający na etapie realizacji dostosowując ją do technologii wykonania sal operacyjnych

(m.in. ścian) oraz do sprzętu medycznego zastosowanego w sali operacyjnej. Wykonawca jest zobowiązany otrzymać jednoznaczną decyzję o lokalizacji interkomu przed montażem.

Interkomy cyfrowe zostaną podłączone do konwerterów sygnału cyfrowego na IP za pomocą kabla UTP cat. 6. Interkomy należy zasilić z dedykowanych zasilaczy medycznych 12 – 24 V AC lub 15 – 35 V DC, maks. 15 W.

Konwertery zostaną umieszczone w szafie PPD.2.1.2 na poziomie P02. Sygnał z konwerterów należy doprowadzić do dekowanego przełącznika sieci LAN Security..

Lokalizację interkomów pokazano na podkładach budowlanych oraz schemacie blokowym.

Na stanowisku pielęgniarskim należy zastosować interkom o parametrach nie gorszych niż:

- Stopień ochrony IP: 20
- Ciśnienie akustyczne: 85 dB / 1 W / 1m, 8Ω
- Wzmacniacz: 700 mW
- Słuchawka: Mikrofon dookólny elektretowy, 50 Ω, gniazdo 4P4C
- Wejście: 2 wejścia cyfrowe dla zmiennych styków
- Wyjście: 2 wyjście cyfrowe typu otwarty dren, maksymalnie 40V DC/1A
- USB: 3 porty USB 2.0 (typ A), WLAN ready
- Wskaźnik połączenia: wielofunkcyjny LED
- Dotykowy ekran TFT 7”, rozdzielczość 800 x 480, 16.777.216
- kolorów, IPS
- Szerokość pasma audio: 16.000 Hz
- Zakres temperatury roboczej: 0 °C do 50 °C (32 °F do 122 °F)
- Zakres temperatury przechowywania: 0 °C do 50 °C (32 °F do 122 °F)
- Wilgotność względna: do 95% bez kondensacji
- Połączenie: Gniazdo RJ 45 ekranowane modułowe
- Zasilanie: PoE (Power over Ethernet) lub zewnętrzne zasilanie 24 VDC
- Pobór mocy urządzenia końcowego: standard IEEE 802.3af
- Protokół Interkomu: IoIP Protokół oparty o UDP/IP
- Protokół IP: IPv4, TCP, UDP, HTTP, RTP, RTCP, DHCP, RTSP, SIP, STUN
- Szybkość transmisji danych: 10/100 MBit/s (Full/Half Duplex)
- Kodeki: G. 711 aLaw,
- G. 711 μLaw,
- G. 722, H. 264, MJPEG, PCM
- Rozszerzenie pamięci: MicroSD

Przy wejściach na oddziały należy zastosować interkom o parametrach nie gorszych niż:

- Panel przedni: Plastik
- Zakres temperatury pracy: –20° C do 70° C
- Zakres temperatury przechowywania: –20°C do 70°C
- Wilgotność względna: do 95% nieskroplone,
- 1 bezpośredniego wywołania.
- Mikrofon: Wszechkierunkowy mikrofon elektretowy, umożliwiający zachowanie maks. 7 m odległości mówienia
- Głośnik: Membrana specjalnego typu dla optymalnej jakości dźwięku, ciśnienie akustyczne: 85dB/1 W/1 m (3,28 st.), 2 x 8 Ω
- Wbudowany wzmacniacz klasy “D” 2,5 W
- Wskaźnik stanu: Trójkolorwa dioda LED
- Wyjście/wyjścia: 2 wyjścia przekaźnikowe i 3 wejścia
- Zakres częstotliwości: 200 do 16 000 Khz
- Połączenie: wtykowe zaciski śrubowe
- IP Uplink/Downlink: ekranowane wtyczki modułowe RJ 45
- Okablowanie: Minimum kat. 5

- Zasilanie poprzez PoE klasy 3 lub zewnętrznego źródła zasilania 12 – 24 VAC lub 15 – 35 V DC
- Protokół IoIP oparty na UDP/IP
- Ethernet: 2 x 10/100 MB/s (pełny dupleks/półdupleks)
- Kamera dane:
- Obiektyw: 2,8 mm, ze stałą ogniskową
- Automatyczna regulacja parametrów nasycenia bieli, barwy, kontrastu oraz jasności
- Regulowany pod kątem do 30° poziomo/ pionowo
- Strumień wideo IP: Rozdzielczość: 320 x 240 lub 640 x 480
- Prędkość odświeżania: do 30 klatek na sekundę
- Protokoły: HTTP, ARP, UDP, TCP, IP, ICMP, DHCP (klient)
- Ethernet: 10/100 MBit/s, tryb pełnego dupleksu/ półdupleksu
- Podświetlenie kamery/ podgrzewacz kamery:
- Możliwość zapamiętywania pięciu klatek wywołanych zdarzeniem na zasadzie „zrzutu ekranu

Na salach operacyjnych należy zastosować interkom o parametrach nie gorszych niż:

- Stopień ochrony: IP 65
- Panel przedni: Plastikowy i osłonięty hermetycznie folią,
- zgodny z normą EN 60601-1
- Mikrofon: Dookólny mikrofon elektretowy umożliwiający rozmowę z odległości maks. 7 m
- Głośnik: Specjalny typ membrany w celu uzyskania optymalnej jakości
- dźwieku, ciśnienie akustyczne: 85 dB/ 1 W/ 1 m, 2 x 8 omów
- Wzmacniacz: Zintegrowany wzmacniacz klasy „D" o mocy 2,5 W
- Wejście: 3 wejścia dla zmiennych styków
- Wyjście: 2 wyjścia przekaźnikowe (styki przełączne) 30 V / 1 A
- Wyjście linii: W celu podłączenia modułu głośnikowego (wraz z funkcją MUTE)
- Wykryw. sabotażu: Przełącznik antysabotażowy (styk „rozwierny")
- Wskazywanie przywoływania: Wielofunkcyjne diody LED (kolory: czerwony, zielony, niebieski)
- Klawiatura: pełna klawiatura alfanumeryczna, podświetlenie w kolorze białym
- Wyświetlacz: LCD, 128 x 64 pikseli, podświetlenie w białym kolorze
- Zgodność: EN 60601-1-2
- Zakres częstotliwości: 200 – 16 000 Hz
- Zakres temperatury roboczej: –20°C do +70°C
- Zakres temperatury przechowywania: –20°C do +70°C
- Wilgotność względna: Maks. 95% bez kondensacji
- Źródło zasilania: Zewnętrzne źródło zasilania 12 – 24 V AC lub 15 – 35 V DC, maks. 15 W
- Okablowanie: rozprowadzane gwiaździście, 2-żyłowe, skręcone

<u>Serwer</u>

Zaprojektowany serwer jest serwerem w pełni IP. Zostanie zlokalizowany w szafie rack systemu Security w serwerowni znajdującej się na poziomie -1. Serwer może obsłużyć minimum 244 abonentów IoIP i SIP. Serwer zostanie dostarczony wraz z oprogramowaniem dedykowanym do systemów interkomowych spełniającym funkcje opisane w następnym rozdziale.

Należy zastosować serwery wraz z oprogramowaniem o parametrach nie gorszych niż:

- Zarejestrowani subskrybenci: IP/SIP: maks. 224
- Połączenia równoległe: rozmowy: maks. 32 połączenia audio w ramach instancji serwera (np. rozmowy, połączenia grupowe/wszystkie lub konferencje):
- połączenia audio typu SIP maks. 112

- Zgodność: CB, RoHS, WEEE, GS, CE, CSAc/us, ULc/us, FCC Class A, VCCI:V3 Klasa A + JIS 61000-3-2, GOST, KC, CCC, CTick, BSMI
- System operacyjny: Linux Debian 8 (64-bitowy)
- Oprogramowanie serwera Intercom: dedykowane oprogramowanie (zainstalowane fabrycznie)
- Prędkość transmisji danych: maks. 1 Gbps
- Zakres temperatury eksploatacyjnej: od +6 °C do +40 °C
- Zakres temperatury składowania: od -25 °C do +60 °C
- Wilgotność względna: od 10% do 85%, bez kondensacji
- Instalacja: montaż w systemie regałowym (1 U na wym. 19")

System będzie wykorzystywał dedykowane okablowanie i przełączniki sieci security.

Funkcjonalność

Zaprojektowany system interkomowy przewiduje następujące funkcje interkomowe:

- Funkcje interkomów DSP
- Funkcje alarmowe
- Funkcje otwarcia przejścia kontrolowanego
- Rozgłoszenie grupowe
- Konferencję.
- Kanały muzyczne
- Kanały radiowe.
- Funkcje stacji głównej.
- Integracja z telefonią VoIP
- Nagrywanie rozmów przez system CCTV

W poniższych punktach opisano szczegółowy sposób działania poszczególnych funkcji interkomowych.

Zastosowanie DSP

Stacje oraz serwer interkomowy będą wyposażone w technologie cyfrowego przetwarzania sygnałów (DSP). Technologia DSP spełnia wiele istotnych funkcji bezpieczeństwa oraz ma znaczący wpływ, na jakość połączeń głosowych w interkomowym systemie bezpieczeństwa i komunikacji. Poniżej przedstawiono wymagane funkcje DSP, które musi realizować serwer interkomowy.

Dzięki funkcji wykrywania aktywności głosu na stacji interkomowej, możliwy jest do wykrycia koniec rozmowy interkomowej, co w następstwie automatycznie zakończy rozmowę interkomową bez potrzeby użycia przycisku na klawiaturze interkomu.

Funkcja audio monitoringu na stacjach wywoławczych z DSP powinna cały czas mierzyć i monitorować poziom hałasu otoczenia w pomieszczeniu wyrażony w dB. Funkcja monitoringu powinna być realizowana za pomocą podłączonego mikrofonu. Jeżeli poziom hałasu w pomieszczeniu przekroczył zaprogramowany próg alarmowy, musi istnieć możliwość zestawiania automatycznego połączenia alarmowego między stacją generująca alarm z wybraną stacji interkomową centralnego stanowiska sterowania (CSS) np. stacją ochrony.

W celu ustalenia, z jakiego powodu połączenie alarmowe zostało wygenerowane za pomocą funkcji audio monitoringu, system interkomowy musi oferować funkcję audio monitoring z funkcją nagrywania głosu. Sygnał audio ze stacji wywoławczej musi być nagrywany minimum kilka sekund przed przekroczeniem progu alarmowego, tzn. przed zdarzeniem alarmowym, w chwili przekroczenia progu alarmowego, aż do momentu odebrania połączenia alarmowego na stacji interkomowej CSS. Po przyjęciu zgłoszenia operator może w trybie ręcznym lub automatycznym odsłuchać nagranie na interkomie a następnie aktywować rozmowę interkomową. Musi być możliwe, aby zmienić ustawienia minimalnego poziomu hałasu (progu

alarmowego), za pośrednictwem stacji interkomowej CSS w sytuacji zmiennych warunków akustyczny wybranych pomieszczeń.

System musi mieć możliwość dostosowania poziom głośności mikrofonu, zarówno dla mikrofonów wewnętrznych i zewnętrznych za pomocą oprogramowania konfiguracyjnego.

System musi prowadzić monitoring poprawności działania nie tylko połączenia interkomu z serwerem, tzw. monitoring linii, ale także poprawne działanie toru połączenia głośnika i mikrofonu. Funkcja testowa poprawności działania głośnika i mikrofonu musi być realizowana za pomocą automatycznej procedury aktywowanej przez serwer. Głośnik musi wysyłać biały szum w zaprogramowanych odstępach czasu, minimalnie, co 1 minutę. Biały szum jest odbierany przez mikrofon. Następnie funkcja DSP analizuje odebrany sygnał (widmo). Uszkodzenie głośnika lub mikrofonu musi być sygnalizowane informacja o uszkodzeniu linii, które musi być wysłane do stacji interkomowej CSS. Dodatkowo musi istnieć możliwość zaprogramowania przekaźnika wbudowanego w stację interkomową, który będzie zmieniał swój stan NO/NC w zależności czy urządzenie działa poprawnie.

W zależności od zmieniającego się poziomu hałasu otoczenia wyrażonego w dB system powinien mieć możliwość automatycznej regulacji głośności stacji interkomowych. Źródłem hałasu mogą być rozmawiające lub krzyczące osoby, głośna muzyka, itd. W przypadku nagłego zwiększania się hałasu otoczenia, moc wzmocnienia głośnika w stacji interkomowej zostanie automatycznie zwiększona a moc wzmocnienia mikrofonu zostanie obniżona. Po obniżeniu poziomu hałasu otoczenia do domyślnej wartości, zmienione ustawienia mocy głośnika i mikrofony zostaną odpowiednio zmienione do wartości domyślnej. Taka funkcjonalność spowoduje, że w stacjach interkomowych nie ma potrzeby ręcznej regulacji głośności.

Funkcje alarmowe

W celu zwiększenia bezpieczeństwa na obiekcie system interkomowy będzie wyposażony z funkcje powiadamiające o alarmie.

System powinien umożliwiać opcjonalne wysłanie cichego powiadomienia alarmowego na grupę wielu odbiorców. Alarm powinien być możliwy do wygenerowania za pomocą różnych urządzeń podłączonych do zacisków wejściowych np. przycisku napadowego lub nożnego oraz za pomocą przycisku na klawiaturze interkomu.

Aktywacja cichego alarmu powinna umożliwiać automatyczny nasłuch akustyczny stacji interkomowej, z której został wygenerowany alarm przez stację interkomową centralnego stanowiska sterowania (CSS). System powinien umożliwiać wysłanie cichego powiadomienia alarmowego na grupę wielu odbiorców w tym samym czasie. Każdy odbiorca alarmu musi mieć możliwość nasłuchiwania, co się dzieje w pomieszczeniu osoby wywołującej alarm w tym samym czasie. Na stacji interkomowej wywołującej alarm mikrofon jest włączony a głośnik jest wyłączony w celu uniknięcia podejrzeń załączania alarmu.

Nasłuch na stacji interkomowej CSS może być uruchomiony automatycznie w chwili wystąpienia alarmu lub ręcznie przez operatora przyjmującego zgłoszenie. Alarm może być odebrany dowolnym przyciskiem na interkomie. Odbiorca w zależności od konfiguracji może nadać komunikat głosowy na stację, która wygenerowała alarm. Musi istnieć możliwość zablokowania tej funkcjonalności. Odbiorca alarmów może odbierać wiele sygnałów alarmowych w tym samym czasie. Na stacji interkomowej inicjalizującej alarm musi być możliwe, aby wyłączyć diodę LED sygnalizującą połączenie głosowe, aby nie wzbudzić podejrzeń. Dodatkowo na wyświetlaczu osoby inicjalizującej alarm musi się wyświetlić informacja o ilości osób, które odebrały alarm.

Jeżeli alarm nie zostanie odebrany przez żadną osobę w domyślnej grupie odbiorców przez zaprogramowany czas, można ustawić przekierowane powiadomienia alarmowego do innej grupy odbiorców. Dodatkowo musi istnieć możliwość zaprogramowania blokady przycisków na interkomie dla grupy odbiorców alarmu. W takiej sytuacji odbiorcy mogą tylko odebrać alarm a nie wykonywać inne operacje. Alarmy muszą mieć różne priorytety. Priorytety określają, które funkcje mogą zostać nadpisane przez wysyłany alarm na stacji CSS, np. przerwanie aktywnej rozmowy, zakończenie odsłuchu rozgłoszenia grupowego.

Funkcje otwarcia przejścia kontrolowanego

W celu lepszej weryfikacji osób poruszających się po obiekcie dla przejść chronionych elementami ryglującymi musi istnieć możliwość otwarcia i zamknięcia danego przejścia z poziomu systemu interkomowego.

System musi posiadać funkcjonalność umożliwiającą przypisanie zaprogramowanego przycisku na stacji interkomowej dla funkcji otwarcia drzwi. Funkcja ta będzie tylko aktywna w momencie aktywnego połącznia stacji wywoławczej ze stacją interkomową w centralnym stanowisku sterowania (CSS). Jeżeli operator przyjmujący zgłoszenie ze stacji wywoławczej stwierdzi, że upoważnia osobę do wejścia na teren obiektu, za pomocą przycisku na interkomowej może otworzyć dane przejście.

Musi być możliwe przypisanie czasu otwarcia przekaźnika sterującego, czas musi być liczony od momentu wciśnięcia przycisku otwarcia na interkomie operatora CSS. Połączenie miedzy stacją nadawczą a stacją CSS musi być automatycznie zakończone po wyborze funkcji otwarcia drzwi. System także musi umożliwiać automatyczne zakończenie rozmowy po zaprogramowanym czasie. Musi być możliwy monitoring otwarcia drzwi za pomocą automatycznego przełączania kierunku mowy od stacji bramowej do stacji głównej. W takiej sytuacji można nasłuchiwać czy interesant otworzył i zamknął drzwi. Głośnik w stacji bramowej jest tej sytuacji wyłączony i interesant nie słyszy, co się dzieje u operatora stacji głównej. Musi być możliwe do zaprogramowanie sterowanie przekaźnika sterującego z funkcja flip flop. Oznacza to, że pojedynczą akcja operatora zamienia tylko raz stan na przekaźnika w zależności od tego, w jakim stanie się on znajduje. W przypadku wielu zgłoszeń, z wielu stacji nadawczych w tym samym czasie, rozmowy powinny być uporządkowane w kolejności zgłoszenia i przetwarzane w kolejności wybranej przez operatora. Dodatkowo musi być możliwe wskazanie stanu otwarcia drzwi na wyświetlaczu interkomu za pomocą sygnału wejściowego, np. kontaktronu. Zgłoszenie ze stacji bramowej powinno być możliwe do wysłania dla wielu odbiorców w tym samym czasie. Musi być możliwe automatyczne przekierowanie połączenia stacji bramowej na inną grupowe odbiorców, jeżeli po zaprogramowanym czasie żaden z operatorów grupy podstawowej nie odbierze zgłoszenia.

Rozgłoszenie grupowe interkomowe

System musi umożliwiać nadawanie komunikatów grupowych na wszystkie interkomy lub wydzieloną grupę odbiorców.

Rozgłoszenie grupowe do wszystkich użytkowników musi być dostępne z każdej stacji interkomowej. Dodatkowo podczas rozgłoszenia grupowego musi istnieć możliwość zakończenia rozgłaszania w trybie szybkiej odpowiedzi do nadawcy rozgłoszenia. Możliwość szybkiej odpowiedzi do nadawcy rozgłoszenia jest szczególnie przydatne dla stacji interkomowych bez wyświetlacza lub ograniczoną klawiaturą.

Musi być możliwe ustawienie indywidualnego dźwięku zapowiadającego rozgłoszenie grupowe dla lepszej identyfikacji rodzaju rozgłoszenia lub docelowej grupy odbiorców. Musi być możliwe ustawienie dźwięku tonowego, dźwięku gong oraz zapowiedzi głosowej (komunikat słowny). Dodatkowo musi istnieć możliwość dodania dodatkowego opisu tekstowego, wyświetlanego na wyświetlaczu interkomów w celu lepszej identyfikacji grupy odbiorców oraz rodzaju i typu rozgłoszenia.

Rozgłoszenie grupowe z funkcją Push To Talk (PTT). Ten typ rozgłoszenia musi być dostępny w kilku wariantach.

Wersja I: Inicjator rozpoczyna rozgłoszenie, następnie wszyscy odbiorcy w grupie słyszą dźwięk informujący o nadchodzącym rozgłoszeniu grupowym. Gdy inicjator rozgłoszenia naciśnie przycisk, aktywuje się mikrofon na stacji inicjatora i można nadawać komunikat. Po zwolnieniu przycisku rozgłoszenie automatyczne zostanie zakończone. W tym trybie żaden z odbiorców nie ma możliwości bezpośredniego oddzwonienia do inicjatora.

Wersja druga rozgłoszenia PTT: Inicjator rozpoczyna rozgłoszenie, następnie wszyscy odbiorcy słyszą dźwięk informujący o rozgłoszeniu. Gdy inicjator naciśnie przycisk, aktywuje się

mikrofon w celu nadania komunikatu. Po zwolnieniu przycisku mikrofon zostanie wyłączony, ale połączenie nie zostaje zakończone. Następnie operator może ustawić opcję szybkiego oddzwonienia. W tym trybie pracy wszyscy odbiorcy rozgłoszenia mogą bezpośrednio oddzwonić do nadawcy za pomocą przycisku szybkiego wyboru bez potrzeby wyboru numer stacji.

Wersja trzecia: Inicjator rozpoczyna rozgłoszenie, następnie wszyscy użytkownicy z grupy słyszą dźwięk informujący o rozgłoszeniu. Gdy inicjator naciśnie przycisk aktywuje się mikrofon w celu nadania komunikatu. Po zwolnieniu przycisku mikrofon zostanie wyłączony, ale połączenie nie zostaje zakończone. Gdy operator kolejny raz naciśnie przycisk PPT może nadać kolejny komunikat grupowy. W tym trybie żaden z odbiorców nie ma możliwości bezpośredniego oddzwonienia do inicjatora.

Dodatkowo system umożliwia realizację zabezpieczenia przed sprzężeniem zwrotnym dla rozgłoszeń grupowych. W celu uniknięcia efektu sprzężenia zwrotnego podczas komunikatów głosowych dla stacji interkomowych, która są umieszczone blisko siebie, system musi zapewniać mechanizmy zabezpieczające. Jednym z mechanizmów musi być zmniejszenie mocy głośników podczas połączeń grupowych. Drugim mechanizmem jest możliwość nagrania komunikatu głosowego z poziomu interkomu a następnie odtworzenie go na wybraną grupę odbiorców. Musi istnieć także możliwość nagrania komunikatu, następnie odsłuchanie nagranego komunikatu grupowego na własnej stacji w celu weryfikacji, możliwość ponownego nagrania i jeżeli nagrany komunikat jest poprawny można go wysłać tak przygotowany komunikat, jako rozgłoszenie grupowe. Nagrany komunikat nie zostanie zapisany w serwerze interkomowym. Ponadto musi istnieć możliwość nagrania komunikatu głosowego z poziomu interkomu a następnie zapisanie tego komunikatu na serwerze interkomowym w celu jego wielokrotnego odtwarzania przy rozgłoszeniach grupowych. Odtworzenie nagranych komunikatów może nastąpić bezpośrednio po wciśnięciu przycisku lub po zaprogramowanym czasie.

Rozgłoszenia grupowe na zewnętrzne systemy PA

System interkomowy musi umożliwiać wysłanie komunikatów grupowych za pomocą wyjść liniowych audio do system PA innych producentów.

Jeżeli do systemu interkomowego podłączony jest zewnętrzny system rozgłoszeniowy PA innego producenta, to musi być koniecznie wygenerowanie opóźnienia rozgłoszenia grupowego do momentu aż kanał głosowy w zewnętrznym systemie PA będzie „wolny". W przeciwnym przypadku, nadany komunikat nie zostanie odebrany przez użytkowników systemu PA.

Dlatego serwer interkomowy musi być tak skonfigurowany, aby oczekiwał na wiadomość z systemu PA, o gotowości do rozgłoszenia komunikatu grupowego. W sytuacji, gdy kanał głosowy w zewnętrznym systemie PA jest zajęty, operator musi usłyszeć dźwięk zajętości. Powyższa funkcjonalność może być realizowana za pomocą przekaźników w systemie PA oraz wejść w systemie interkomowym. Dopuszczalna jest także realizacja softwarowa.

Konferencje

System interkomowy musi umożliwiać połączenie typu konferencja dla wielu stacji interkomowych jednocześnie. System musi umożliwiać ustawienie maksymalnego czasu trwania konferencji. Po upłynięciu zaprogramowanego czasu konferencja jest rozłączana automatycznie.

System interkomowy musi umożliwiać podczas normalnej rozmowy interkomowej dwóch użytkowników zaproszenie do rozmowy innych użytkowników, tworząc tzn. konferencję. Użytkownik chcący zaprosić kolejnych użytkowników musi wybrać kod a następnie numery danych użytkowników, którzy mają uczestniczyć w konferencji.

System powinien umożliwiać zestawienie konferencji w trybie Simplex. Konferencja w trybie Simplex oznacza tryb, gdzie tylko jedna osoba może mówić (załączony mikrofon) a pozostałe mogą tylko słuchać (wyłączony mikrofon, załączony głośnik). Ten tryb konferencji może być prowadzony w trybie Push To Talk (PTT). W trybie PTT osobą trzymająca wciśnięty przycisk ma załączony mikrofon. Inną dostępna opcją sterowania jest tryb przełączania stacji nadawczej za

pomocą pojedynczego wciśnięcia przycisku. W tym trybie osoba wciskając przycisk włącza swój mikrofon i może mówić bez potrzeby trzymania przycisku. Musi istnieć możliwość zablokowania opcji rozłączania się od konferencji pojedynczych osób.

System musi umożliwiać zaprogramowanie predefiniowanych konferencji. W takim przypadku nie ma potrzeby za każdym razem zapraszać kolejnych uczestników do konferencji. Lista podstawowych użytkowników jest stała, ale nadal podczas konferencji można „dopraszać" kolejnych użytkowników.

Do każdego odbiorcy konferencji możliwe jest zaprogramowanie wyjścia przekaźnikowego, aktywnego tak długo jak długo jest on podłączony do konferencji. Musi istnieć możliwość odtworzenia domyślnego lub indywidualnego dźwięku przed rozpoczęciem konferencji. Ponadto system musi mieć możliwość przypisania tekstu z opisem konferencji. Tekst musi być wyświetlany na wyświetlaczu interkomu dla lepszej identyfikacji konferencji.

Musi być możliwe określenie minimum kilku poziomów priorytetów na konferencje, aby konferencja z wyższym priorytetem była generowana automatycznie. Nadanie priorytetów konferencji spowoduje, że stacje interkomowe odbiorców będące w różnych stanach pracy takich jak aktywna rozmowa, aktywne rozgłoszenie grupowe, zostaną podłączeni do konferencji lub też nie. W sytuacji automatycznego połączenia do konferencji poprzedni stan kanału rozmównego np. aktywna rozmowa nie zostanie zakończona, ale zawieszona. Po zakończeniu udziału w konferencji dana rozmowa zostanie przywrócona automatycznie.

Konferencja typu Duplex. Musi istnieć możliwość aktywacji konferencji wielu użytkowników, gdzie wszyscy użytkownicy mogą mówić i słuchać w tym samym czasie bez potrzeby kontroli przełączanie mowy. Mikrofon i głośnik wszystkich użytkowników konferencji jest załączony cały czas.

Powyższy typ konferencji może być skonfigurowany w dwóch trybach pracy. Predefiniowany tzn. lista osób, które biorą udział w konferencji jest z góry ustalona. Tryb kodu wybieranego za pomocą przycisku szybkiego wybierania. Konferencja ze wszystkimi użytkownikami jest zestawiona automatycznie i nie ma potrzeby manualnego dopraszania użytkowników.

Kolejnym typem konferencji jest konferencja typu party linie. Konferencja w trybie party linie polega na zestawieniu konferencji przez jednego użytkownika a następnie ręcznym podłączaniu się użytkowników, którzy chcą wziąć udział w konferencji.

Kanały muzyczne

Każdy użytkownik interkomu opcjonalnie może mieć możliwość połączenia się z programem muzycznym, gdy stacja jest stanie bezczynności. Jeżeli stacja stacje się aktywna, np. przychodzące połącznie, muzyka musi się automatycznie wyciszyć na okres trwania rozmowy, rozgłoszenia konferencji. System powinien także umożliwiać automatyczne załączanie przekaźnika dla każdej stacji interkomowej, która bierze udział w odsłuchu kanału muzycznego.

Przełączanie kanałów muzycznych, powinno być możliwe za pomocą jednego przycisku. Powinno być także możliwe do skonfigurowania przełączanie powinno być zapętlone czy odtwarzanie muzyki zostanie zakończone po wybraniu ostatniego kanału muzycznego.

Dodatkowo powinna istnieć możliwość automatycznego załączenie kanału muzycznego na wybranych stacjach po resecie serwera interkomowego.

Producent powinien mieć w ofercie serwer interkomowy, do którego musi być możliwe wprowadzenie sygnału muzycznego lub radiowego za pomocą wejścia liniowego wbudowanego bezpośrednio w centralę interkomową, za pomocą karty audio oraz za pomocą modułu interkomowego analogowego i cyfrowego.

Powinno być możliwe używanie sygnałów muzycznych i radiowych, jako informacja w trakcie oczekiwania na połączenie lub rozgłoszenie alarmowe.

Każdy użytkownik interkomu powinien mieć możliwość do osłuchu minimum 40 programów muzycznych.

Kanały radiowe

Opcjonalnie powinno być możliwe dla każdego użytkownika słuchanie do maksymalnie 40 kanałów radiowych wybieranych selektywnie. Podczas słuchania, użytkownik stacji interkomowej powinien być w stanie korzystać z innych funkcji interkomu takich jak inicjowanie lub odbieranie rozmów lub nasłuchiwanie rozgłoszeń grupowych, itd. W przypadku konferencji radiowej użytkownik powinien mieć możliwość usłyszeć informacje, jak również je nadać. Powinno być możliwe przypisanie tych uprawnień dla konkretnych na użytkowników systemu i kanału radiowego. Powinno być możliwe ustawienie konkretnym użytkownikom, automatyczne podłączony do określonego kanału konferencyjnego, gdy serwer interkomu zostanie ponownie uruchomiony. Na wyświetlaczu użytkownika połączonego z kanałem radiowym (w zależności od typu wyświetlacza) powinny ukazać się istotne informacje na temat stacji radiowej oraz o aktualnym stanie w konferencji radiowej. System powinien także umożliwiać automatyczne załączanie przekaźnika dla każdej stacji interkomowej, która bierze udział w odsłuchu kanału radiowego

Integracja z centralą telefoniczną

Do integracji zostanie wykorzystana technologia SIP TRUNK.

Realizacje integracji z centralą telefoniczną przewidzianą za pomocą odpowiedniej licencji oprogramowanie systemu interkomowego.

Oprogramowanie, która pozwala na integrację różnych standardów VoIP, takich jak SIP lub IAX2 bezpośrednio w serwerze interkomowym. Poprzez zintegrowane oprogramowanie możliwa jest prosta konfiguracja zdalna.

Połączenie integrujące System Interkomowego z centralą telefoniczną łączy obydwa systemy w jedną platformę użytkownika. Połączenia mogą być ustanawiane w obydwu kierunkach, wraz z komunikatami na wyświetlaczu. Jedno połączenie fizyczne dostarcza kilka równocześnie działających kanałów mowy poprzez wykorzystanie najnowocześniejszych kodeków. Dostępne są łącza Trunk do różnych serwerów VoIP wiodących producentów.

Zainstalowane oprogramowanie będzie pozwalało na łącze wielokrotne SIP typu "trunk" na 8 kanałów.

Nagrywanie rozmów

Nagrywanie rozmów interkomowych jest istotną cechą całego systemu bezpieczeństwa. Funkcja dotyczy zarówno rozmów interkomowych, jak i rozgłaszanych komunikatów grupowych. Połączenie współczesnych technologii umożliwia nagrywanie obrazu wideo i dźwięku audio wysokiej jakości oraz synchronizację tych dwóch sygnałów pochodzących z dwóch niezależnych strumieni. Takie rozwiązanie zapewnia idealny materiał dowodowy w sytuacjach spornych. Za pomocą aplikacji programowej, system umożliwia rejestrowanie, odtwarzanie i eksportowanie obrazu i dźwięku w jednym pliku. W przypadku nawiązania połączenia głosowego z punktu alarmowego z obsługą, np. z pomieszczeniem ochrony, rozmowa interkomowa oraz przesyłany obraz z kamery CCTV powinien zostać zarchiwizowany i synchronizowany. Aplikacja na serwerze interkomowym umożliwia współpracę z systemem CCTV za pomocą protokołów integracyjnych w technologii IP, co jest istotnym warunkiem dla systemów rozproszonych w różnych lokalizacjach. Integracja systemów zapewnia możliwość nagrania rozmowy w technologii lipsync wykorzystując strumień wideo pochodzący z serwera CCTV i strumień audio pochodzący z serwera interkomowego. Integracja programowa pomiędzy systemami dodatkowo pozwala zarządzać rozmową, rozpoczynać lub kończyć rozmowę interkomową korelując połączenie głosowe z obrazem z kamery systemu CCTV przełączając obraz automatycznie podczas zdarzenia. Dźwięk audio jest zapisywany w oryginalnym kodeku G.722, co zapewnia doskonałą jakość dźwięku HD w paśmie częstotliwości do 7kHz. W proponowanym rozwiązaniu strumień audio jest rejestrowany wraz z przypisanym strumienie wideo na jednym rejestratorze.

4.1.7 System CCTV

Założenia ogólne

Dla potrzeb Szpitala zaprojektowano system telewizji dozorowej w technice IP. Rozwiązanie to pozwala na wprowadzenie w pełni systemu zarządzania urządzeniami i ich konfiguracją jak również dostępem do poszczególnych funkcji systemu oraz umożliwia integrację z innymi systemami opartymi na architekturze IP (instalacje wideointerkomowe, kontroli dostępu oraz sygnalizacji włamania i napadu). System CCTV oparty o serwer i kamery stanowi zintegrowaną platformą IP. Platforma zapewnia możliwość zarządzania zdarzeniami z centrum monitorowania. System składa się z urządzeń w postaci serwerów wizyjnych, monitorów oraz kamer IP. Architektura systemu jest otwarta i oparta na transmisji danych za pomocą LAN, dzięki temu umożliwia tworzenie rozproszonych systemów. W ramach tego rozwiązania przedstawiono w dalszej części niniejszego opracowania opisano instalację telewizji obserwacyjnej pacjenta. Zaprojektowana instalacja telewizji dozorowej zapewnia obserwację:

- Fragmentów ciągów komunikacyjnych – kamery kopułowe wandaloodporne 4 mp. ze zmienną ogniskową 2.8-12mm;
- Hol wejściowy oraz wejścia/wyjścia – kamery kopułowe wandaloodporne ze zmienną ogniskową 2.8-12mm;
- Recepcja – kamery kopułowe wandaloodporne ze zmienną ogniskową 2.8-12mm;
- Windy - kamery kopułowe wandaloodporne dyskretne ze stałą ogniskową 2.8 mm;
- PZT: wejścia do budynku, wjazdy w tym wjazd na SOR, strefa placu zabaw, strefa parkingu za pomocą kamer obrotowych – kamery 3mpix typu bullet oraz kamery 3mpix typu PTZ

System dozoru składa się z kamer stacjonarnych kopułowych, stacji klienckiej z pulpitem sterowniczym i monitorów LCD, serwerów wizyjnych zlokalizowanych w pomieszczeniu serwerowni, wydzielonej sieci LAN oraz oprogramowania nadzorczego. W systemie dozorowym będą występowały martwe strefy – głównym celem jest obserwacja wejść i wyjść.

Serwer

Zaprojektowano system zbudowany w architekturze klient- serwer, który będzie zapewniał hierarchiczną strukturę serwerów, w której można wyróżnić serwer centralny, tzw. serwer master, który zarządza główną bazą danych, zawierającą wszystkie informacje o systemie i konfiguracji komponentów platformy oraz serwerach slave. Serwer master autoryzuje użytkowników i nadaje dostęp do platformy na podstawie predefiniowanych praw dostępu użytkownika oraz ustawień strefy bezpieczeństwa otrzymywanych w czasie logowania z poziomu stacji operatorskiej.

Serwer master zarządza następującymi komponentami platformy:

- grupami użytkowników oraz użytkownikami,
- alarmami z poszczególnych serwerów
- makrami,
- uprawieniami poszczególnych grup użytkowników,
- układami widoków, multi-widoków wraz z przypisanymi do nich urządzeń z poszczególnych serwerów slave,
- sekwencjami kamer,
- harmonogramami nagrywania i archiwizacji,
- wtyczkami (Plug-in) odpowiadającymi za komunikację pomiędzy platformą, a systemami firm trzecich, takimi jak zewnętrzna analityka wideo, system ochrony obwodowej, itd.,
- modułem API HTTP łączącym platformę z dowolną aplikacją lub interfejsem, który został stworzony z jego wykorzystaniem w celu integracji z platformą,
- przydzielonymi kamerami i koderami oraz archiwizowanie wideo / audio,
- urządzeniami zewnętrznymi np. audio, wejście, wyjścia, porty szeregowe; sterowanie PTZ.

Serwery slave zarządzają:

- przydzielonymi kamerami i koderami oraz archiwizowanie wideo/audio,
- urządzeniami zewnętrznymi, np. audio, wejście, wyjścia, porty szeregowe; sterowanie PTZ,
- przesyłaniem wideo i audio przez sieci lokalne i rozległe (LAN, Internet) ze źródła video (kamera, koder) do miejsca docelowego (np. aplikacji klienckiej).

Aplikacja serwerowa platformy musi wspierać architekturę 64-bitową w celu zapewnienia maksymalizacji wykorzystania zasobów serwerów.

Zaprojektowany system musi gwarantować najwyższy poziomu bezpieczeństwa danych w warstwie sprzętowej serwera, usługi systemu operacyjnego, aplikacyjnej – przez możliwość wdrożenia w systemie serwera redundantnego, detekcję sabotażu punktu kamerowego, watchdog aplikacji oraz redundancję sprzętową.

Watchdog usługi serwerowej platformy – w celu eliminacji negatywnego wpływu innych aplikacji współdzielących system operacyjny aplikacja serwera będzie realizowana na bazie usługi systemowej Watchdog, której celem jest monitorowanie usługi serwerowej i weryfikację:

- prawidłowego niezakleszczonego stan usługi serwerowej,
- prawidłowego działania macierzy dyskowej RAID,
- prawidłowego działania bazy danych.

W przypadku wykrycia nieprawidłowości usługa serwerowa jest restartowania w celu uniknięcia błędnego funkcjonowania części platformy w dłuższym czasie, co mogłoby spowodować brak możliwości nagrywania w przypadku serwerów rejestrujących lub braku możliwości podglądu obrazów na żywo, interaktywnej obsługi sytemu w przypadku stacji operatorskich.

Zaprojektowany system CCTV musi zapewniać sprzętowe zabezpieczenie struktury danych video, audio oraz meta danych poprzez zastosowanie technologii RAID 10 w przypisanej do serwera macierzy dyskowej.

Należy zastosować serwery o parametrach technicznych nie gorszych niż:

- System operacyjny 64-bit
- Dysk twardy SSD SATA III 64 GB
- Konfiguracja dysków twardych do 8 dysków(opcjonalnie Raid 5 lub Raid 6)
- Pojemność zapisu do 64TB (58TB skutecznego zapisu przy Raid 5)
- Procesor 8M Cache, 3.50GHz
- Pamięć 8GB Dual Channel DDR3 EEC RAM (2x 4GB)
- Interfejs sieciowy 2 x Gigabit Ethernet RJ-45 (10/100/1000 MB/s)
- Typ obudowy 2U 19-calowy montowanie typu rack
- Moc wejścia 100-240VAC,50/60Hz 5A
- Moc zasilacza 650W
- Temperatura pracy 5° C - 40° C (41°F - 104°F)
- Temperatury przechowywania -40° C - 65° C (-40°F - 149°F)

Serwery należy doposażyć w dedykowane przez producenta dyski 8TB o parametrach nie gorszych niż:

- Bufor do obsługi 256 Mb
- Prędkość obrotowa (RPM) 7200
- Średnia latencji (ms) 4.16
- Interfejs SATA 6Gb/s
- Szybkość transmisji interfejsu (MB/s, max) 600
- Czas wyszukiwania 8.6 ms
- Obciążanie/rozładowywanie cykli (przy 40°C) 600,000
- MTBF (M godz.) 2.5

- AFR 0.44% (2TB,4TB,6TB) / 0.35% (8TB,10TB)
- Ciągłość pracy 24h/ 7
- Typ napędu 3,5 -calowy wewnętrzny dysk twardy
- Temperatura otoczenia podczas pracy od 5° do 60° C
- Wibracje (G RMS, 5-500 Hz) 0.67 (XYZ)

Stacje klienckie

Główne stanowisko monitorowania zaprojektowano na poziomie P00 w pom. ochrony nr 0.819. Stanowisko będzie się składało z dwóch jednostek operatora o wysokości 2U wyposażonych w kartę graficzną typu QUAD(4xVGA/DVI) oraz ośmiu monitorów 32" wyposażonych w matrycę S-IPS przystosowanych do pracy 24/7. W pomieszczeniu ochrony będą znajdować się tylko monitory oraz klawiatura, myszka i pulpit sterowniczy. Jednostki klienckie zostaną umieszczone w szafie rackowej security w PPD.0.2 (szafa nr PPD.0.2.2). W pom. ochrony należy przewidzieć konwertery HDMI/Ethernet na potrzeby monitorów oraz konwertery USB/Ethernet na potrzeby myszek, klawiatur, paneli obsługi, itp. Konwertery powinny być dostarczone wraz z zasilaczami, należy je zasilić napięciem z obwodów gwarantowanych.

Należy zastosować stacje klienckie o parametrach technicznych nie gorszych niż:

• Dysk twardy	SSD SATA 3 64 GB
• System operacyjny	64-bit
• Pojemność zapisu	Do 40 TB 3,5 calowych dysków twardych
• Procesor	8M Cache, 3.6 GHz
• Pamięć	16 GB DDR3 Non-ECC RAM (4x4 GB)
• Interfejs sieci	Podwójny Gigabit Ethernet RJ-45 (10/100/1000 MB/s)
• Wyjście wideo	2 x DVI / 1 x DisplayPort
• Temperatury pracy	5° C - 40° C (41°F - 104°F)
• Temperatury przechowywania	-40° C - 65° C (-40°F - 149°F)
• Typ obudowy	2U 19-calowy montowanie typu rack

Drugie stanowisko operatora zostanie zlokalizowane w pomieszczeniu ochrony 0.043 części SOR. Stanowisko zostanie wyposażone w stację typu desktop z dwoma monitorami 24".

• System operacyjny	64-bit
• Dysk twardy	SSD DRIVE SATA 3 64GB
• Pojemność zapisu	1 x 3.5 cala SATA Dysk twardy (opcjonalnie)
• Procesor	8M Cache, 3.60 GHz
• Pamięć	16 GB DDR3 Non-ECC RAM (4 x 4GB)
• Interfejs sieci	Podwójny Gigabit Ethernet RJ45 (10/100/1000 MB/s)
• Wyjście wideo	2 x DVI / 1 x DisplayPort
• Typ obudowy	Desktop / Tower
• Temperatury działania	5° C - 40° C (41oF – 104oF)
• Temperatury przechowywania	-40° C - 65° C (-40oF – 149oF)

Założenia ogólne dla telewizji „ogólnej”

Dla potrzeb ogólnego CCTV zaprojektowano 244 kamer.

W budynku 207 szt. kamer kopułkowych 4mpix w obudowach wandaloodpornych. Kamery należy montować do sufitu podwieszanego. W przypadku kamery przy wejściu do serwerowni należy zamontować kamerę na wysokości ok 1,8m, tak aby na rejestrowanym obrazie widoczna była twarz osoby wchodzącej do pomieszczenia.

Na elewacji budynku 25 kamer 3mpix typu bullet z inteligentną analizą obrazu w kamerze oraz 1 kamera 3mpix typu PTZ z inteligentną analizą obrazu w kamerze oraz zintegrowanym oświetlaczem podczerwieni o zasięgu do 200m. Kamery montować na wysokości 3-3,5m.

Na słupach na terenie parkingów 4 kamery 3mpix typu bullet z inteligentną analizą obrazu w kamerze oraz 3 kamery 3mpix typu PTZ z inteligentną analizą obrazu w kamerze oraz zintegrowanym oświetlaczem podczerwieni o zasięgu 200m. Do kamer zlokalizowanych poza budynkiem jako medium transmisyjne zostanie wykorzystany światłowód SM podłączony do przemysłowego media konwertera z opcją zasilania PoE (szczegóły wg projektu LAN). Kamery montować na wysokości 3-3,5 m.

Rozmieszczenie kamer pokazano w części rysunkowej.

Jako kamery kopułkowe należy zastosować kamery o parametrach nie gorszych niż:

- Sensor obrazu przetwornik 1/3” typu CMOS
- Minimalne naświetlenie 0.1 lux kolor, 0.01 lux (cz/b), 0 lux z podświetleniem IR
- Szybkość migawki 1/3 s do 1/10,000 s
- Obiektyw zmiennoogniskowy 2,8 do 12 mm, F1. 4
- Automatyczna przysłona DC
- Tryb dzień/noc filtr IR-cut z możliwością demontażu (ICR)
- Podświetlanie IR 24 el., 850 nm
- Odległość skuteczna podświetlania IR do 30 m
- WDR 120 dB
- Udoskonalenie obrazu BLC/ 3D DNR / ROI
- Balans bieli ręczny, AWB1, AWB2, blokada WB, lampa fluorescencyjna, lampa żarowa, światło ciepłe lub naturalne
- Typ H.264 profil główny
- Ilość klatek
- strumień główny: 32kb/s~16384kb/s
- strumień podrzędny: 32kb/s~8192Mb/s
- Maks. rozdzielczość 2688 x 1520
- Przepływność 2688 x 1520 (20/20 kl./s),
- Zestaw funkcji inteligentnych:
- Wykrycie przekroczenia linii przekroczenie wstępnie określonej linii wirtualnej
- Wykrycie wtargnięcia wtargnięcie na wstępnie określony obszar wirtualny
- Detekcja ruchu - 8 zdefiniowanych przez użytkownika, prostokątnych masek; nastawne

  poziomy wykrycia, czułość oraz interwały czasowe
- Sygnalizacja sabotażu wł./wył./zaprogramowana
- obsługa kart pamięci typu SD/SDHC/SDXC o pojemności maksymalnie 128 GB
- Standardy ONVIF (Profil S, Profil G), PSIA, CGI
- autoryzacja użytkownika, znak wodny, filtrowanie po adresie IP, anonimowy dostęp, strumieniowanie kodowane

- Temperatura robocza -30 C do 60 C
- Wilgotność względna 90% lub mniej (bez skroplenia)
- Klasa szczelności IP66
- Odporność na uderzenia IK10

Jako kamery typu bullet należy zastosować kamery o parametrach nie gorszych niż:

- Czułość przetwornika kamery: kolor: 0.05 Lux , B/W: 0.005 Lux , 0 lux (IR wł.)
- Funkcje : WDR 120 dB ,Defog , HLC , BLC
- Obiektyw Autofocus 2.8-12 mm
- Przetwornik 3 Mpx 1/2.8" Progressive Scan CMOS
- Rozdzielczość :FullHD @60 kl/s , 2048 x 1536 @ 45 kl/s
- Wbudowany promiennik 50 m
- Zakres temperaturowy pracy :--30 °C – 60 °C (-22 °F – 140 °F)
- Pyło-/wodoodporność IP66
- Wandaloodporność IK10
- Wbudowana analiza obrazu : Detekcja przekroczenia linii, detekcja wtargnięcia, wejście na obszar, wyjście z obszaru , bagaż bez dozoru, usunięcie obiektu , Detekcja twarzy , zliczanie obiektów (liczba obiektów wchodzących i wychodzących jest liczona oraz wyświetlana na ekranie w czasie rzeczywistym)

Na parkingu zaprojektowano kamery obrotowe PTZ o wysokiej czułości przetwornika z wbudowanymi promiennikami IR o oraz obiektywach umożliwiających rozpoznanie osób na dużych odległościach. Kamery te wykonują przejście po predefiniowanych pozycjach, tzw. presetach, przez co zapewniają obserwację rozległych terenów. Presety mogą być wspomagane przez wykorzystanie algorytmów obrazu oferowanymi przez system CCTV w celu automatycznej detekcji sytuacji alarmowych i ich zapis w bazie danych systemu CCTV w celu późniejszej weryfikacji lub alarmowania na żywo operatorów.

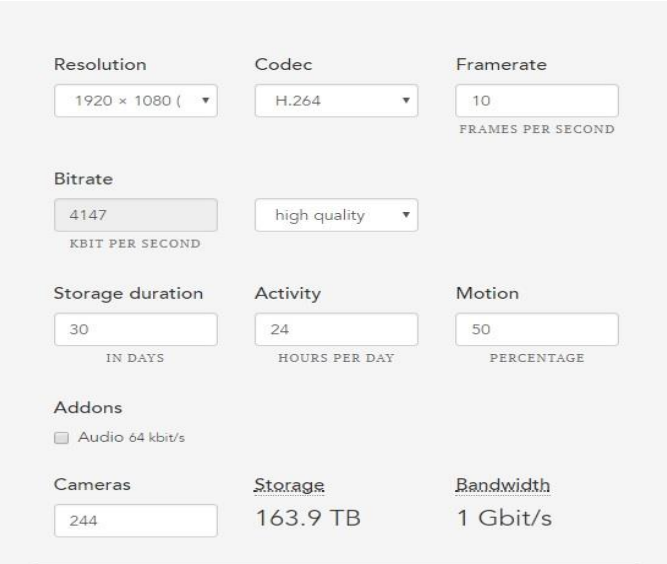
Jako kamery typu PTZ należy zastosować kamery o parametrach nie gorszych niż:

- Czułość przetwornika kamery: kolor: 0.05 Lux , B/W: 0.01 Lux , 0 lux (IR wł.)
- WDR 120 dB ,Defog , HLC , BLC
- Przetwornik 3 Mpx 1/3" Progressive Scan CMOS
- Obiektyw Autofocus Zoom 36x (ogniskowa 4.5-162mm)
- Rozdzielczość : 2048 x 1536 przy 30 kl/s
- Wbudowany promiennik 200 m
- Pyło-/wodoodporność IP66
- Wandaloodporność IK10
- Zakres temperaturowy pracy :-40 °C – 65 °C
- Ilość presetów/ tras: 300 presetów ,10 tras
- Wbudowana funkcja śledzenie obiektów

- Wbudowana analiza obrazu: Detekcja przekroczenia linii, detekcja wtargnięcia, wejście na obszar, wyjście z obszaru, bagaż bez dozoru, usunięcie obiektu, detekcja twarzy, zliczanie obiektów (liczba obiektów wchodzących i wychodzących jest liczona oraz wyświetlana na ekranie w czasie rzeczywistym).

Zapis obrazu i zasilanie

W projekcie przyjęto następujące parametry rejestracji obrazu: czas rejestracji 30 dni z poklatkowością 10kl/s przy rozdzielczości 1920x1080p z zastosowaniem kodeka H.264. Poniżej znajdują się szczegółowe wyliczenia dotyczące zapisu oraz przepustowości sieci:



Z uwagi na fakt, że Inwestor wymaga zapisu w RAID 10 oraz zapasu miejsca pod rozbudowę serwery należy doposażyć w dedykowane przez producenta systemu dyski o łącznej pojemności nie mniejszej niż 384 TB.

Kamery pracujące w systemie telewizji CCTV ogólnej włączone są w wydzieloną fizycznie sieć LAN, mają także osobne przełączniki oraz serwery.

Zasilanie kamer wewnętrznych oraz kamer umieszczonych na elewacji zrealizowano poprzez sieć (PoE). Kamery wyniesione poza budynek wymagają zasilania z dedykowanych przemysłowych media konwerterów (szczegóły wg projektu LAN).

Poszczególne elementy instalacji: zasilacze, przełączniki, panele krosowe zamontowane będą w szafach teleinformatycznych RACK 19” części security zlokalizowanych w pomieszczeniach teletechnicznych. Wymagania instalacyjne odnośnie klasy łączy i kategorii urządzeń opisano w projekcie instalacji okablowania strukturalnego.

Serwer i przełącznik rdzeniowy sieci telewizji zaprojektowano w szafach w serwerowni. Urządzenia instalacji telewizji zasilane są z obwodów gwarantowanych UPS (230V/50Hz). Z uwagi na zakładaną możliwość zamiany funkcji transmisji oraz fizycznych przełączeń pomiędzy siecią strukturalną i siecią telewizji, należy po zakończeniu robót montażowych przyprowadzić pomiary parametrów sieci wg PN-EN50346 dla klasy EA kanału transmisji w zakresie okablowania miedzianego oraz OF300 dla okablowania światłowodowego.

Interfejs

W celu podniesienia bezpieczeństwa zaprojektowany system umożliwia tworzenie elastycznego interfejsu użytkownika szytego na miarę potrzeb, który zapewni intuicyjną pracę oraz

ekspresowy czas reakcji. Praca operatora będzie wspierana przez następujące cechy interfejsu systemu:

- w pełni edytowalne przyciski ekranowe rozmieszczane w dowolnym miejscu poszczególnych widoków zapewniające możliwość przełączania pomiędzy widokami lub wyzwalania zaawansowanych makr oferujących możliwość wielopoziomowych akcji
- aktywowanie dowolnego makra w tym presetów kamer PTZ po kliknięciu kursorem myszy na predefiniowanym transparentnym regionie obrazu na dowolnym widoku powiązanej kamery stacjonarnej,
- wsparcie dla kontrolera USB z joystickiem do kontrolowania funkcji PTZ ruchomych punktów kamerowych oraz możliwość kontrolowanie kamer PTZ z poziomu panelu w oprogramowaniu,
- obsługa cyfrowych modułów I/O aktywowanych z poziomu dedykowanych przycisków ekranowych lub automatycznie przez egzekucję reguł makr,
- jednoczesny dostęp do 4 wskazanych kamer jednocześnie z obsługą PTZ z poziomu przeglądarki internetowej,
- jednoczesny podgląd obrazu archiwalnego z minimum 48 kamer jednocześnie na jednej stacji operatorskiej,
- dostęp do serwerów z poziomu urządzeń mobilnych (iOS, Android) pozwalający na oglądanie bieżących widoków z kamer, sterowanie funkcjami PTZ oraz przechwytywanie zdjęć ze wskazanych momentów obserwowanego obrazu,
- swobodne nadawanie przez administratora systemu hierarchicznych uprawnień każdemu operatorowi lub grupie operatorów korzystających z odpowiednich dla nich zasobów systemu takich jak dostęp grup użytkowników do urządzeń, funkcjonalności urządzeń, widoków, reguł makr domyślnego widoku wyświetlania,
- edytowalne reguły makr budowane w oparciu o instrukcje warunkowe aktywowane krzyżowo przez wszelkie zasoby systemu, systemów integrowanych oraz funkcjonalności systemu,
- wsparcie 4 i więcej monitorów o dowolnej przekątnej ekranu w ramach każdego stanowiska operatorskiego, w tym wirtualnego kontrolera z matrycą dotykową oraz klawiaturą numeryczną,
- definiowanie widoków (wyświetlanie na pojedynczym monitorze) oraz multi-widoków (wyświetlanie na wielu monitorach) o różnej zawartości poszczególnych paneli (np. obraz na żywo, odtwarzanie, zegar, adres URL, lista zdarzeń, przycisk funkcyjny, mapa obiektu, sterowanie PTZ), dowolnym rozmiarze oraz położeniu w ekranie monitora,
- zbliżenie cyfrowe wybranego fragmentu obrazu bez utraty podglądu na pierwotny zakres obserwowanej sceny,
- wybór kamery do aktualnego podglądu przez przeciągniecie ikony kamery z mapy synoptycznej,
- wskazanie materiału blokowanego przed nadpisaniem,
- rozpoczęcie nagrywania po detekcji ruchu definiowanej dla dowolnego obszaru kamery,
- zmiana atrybutów zapisu przypisana do aktywnego profilu,
- odtwarzanie ostatnich kilkunastu sekund nagrania bezpośrednio z widoku kamery będącej aktualnie w trybie podglądu bieżącego obrazu po kliknięciu prawym przyciskiem myszy,
- dynamiczna zmian trybów, parametrów nagrywanie poprzez makra jako reakcja na dowolne zdefiniowane przez użytkownika zdarzenie w systemie,

- zmiana parametrów nagrywaniu w oparciu o kalendarz tygodniowy lub roczny dedykowane szczególnie dla wydarzeń niepowtarzalnych w terminarzu jak imprezy masowe,
- eksport materiału z wielu serwerów jednocześnie do jednego pliku z materiałem archiwalnym,
- wybór kamery do podglądu archiwalnego przez przeciągniecie ikony kamery z mapy synoptycznej,
- funkcjonalność zoomo`walnych map umożliwiających wykorzystanie w wizualizacji obiektów map wektorowych dzięki czemu na jednej tylko mapie wysokiej rozdzielczości można umieścić elementy znajdując się na całym chronionym obiekcie, które będąc scrollowane zapewniają bardzo szybkie przejście od podglądu ogólnego obrysu obiektu do wysokiego poziomi szczegółowości np. do poziomu danego pomieszczenia,
- programowa korekcja zniekształceń obrazu dla wszystkich obsługiwanych kamer w tym min dla kamer analogowych,
- obsługa kamer 360 stopni typu rybie oko – odbywa się przez możliwość rozłożenia jednego strumieni kamery dowolnego producenta na trzy widoki w dedykowanych panelach umożliwiające: podgląd panoramiczny, sferyczny oraz podgląd na obszar wybrany przez obrót ePTZ i przez wskazanie przez operatora w poglądzie panoramicznym oraz sferycznym przy czym obserwowany na tym panelu obraz jest zaznaczany obwódką w celu łatwej orientacji w obserwowanym materiale,
- możliwość precyzyjnej lokalizacji zdarzenia na skorelowanej mapie synoptycznej np. poprzez wskazanie przez podświetlenie transparentnych wielopoligonowych obszarów wizualizujących miejsce wykrycia alarmu,
- możliwość korelacji dowolnej rekcji systemu np. przełączenie trybu nagrywanie, wyzwolenie presetu kamery, przesłanie sygnału do sytemu integrowanego, aktywacja analizy obrazu dla wybranej kamery lub grupy kamer, wyzwalanego poprzez transparentny wielopoligonowy obszar,
- system ma dawać możliwość automatycznego wskazanie obrazu z kamer obserwujących dany interesujący obszar obiektu bez konieczności znajomości przez operatora nazw, grupy kamer oraz ich hierarchii – funkcjonalność ta zwiększa ergonomię i szybkość pracy operatora,
- możliwość wysłania emaila z dołączanym zdjęciem prezentującym zdarzenie alarmowe poprzez wykorzystanie przez silnik makr wraz z możliwością tworzenia generycznych makr – przechwytywanie wielu zdarzeń przez jedno generyczne makro,
- alarmowanie o opóźnieniu w transmisji materiału z kamer – jest kluczowe w systemach wykorzystujących punkty kamerowe do: sterowania automatyką / weryfikacji procesów technologicznych, obsługi systemów rozproszonych. System musi alarmować operatora w przypadku wystąpienia opóźnienia w transmisji obrazu powyżej 500 ms. System musi zapewniać operatorowi jasny komunikat, np. czerwony krzyż oraz możliwość obsłużenia zdarzenie poprzez silnik makr.

Algorytmy

System musi zapewniać możliwość rozszerzenie bezpieczeństwa obiektu poprzez implementację algorytmów inteligentnej analizy obrazu. System pozwoli na migrację funkcji analitycznych w obszarze zasobów systemu oznaczającą brak konieczności stosowania wyspecjalizowanych kamer dedykowanych do realizacji tejże analizy zawartości obrazu oraz możliwość wykorzystywania jednej kamery do wykonywania wielu analiz (minimum 5 różnych typów analiz jednocześnie) lub wdrożenie analizy obrazu dla istniejących analogowych lub sieciowych punktów kamerowych.

W celu sprawniejszego wyszukiwania zdarzeń algorytmy muszą:

- umożliwiać analizę danych post factum pozwalająca na wykonanie analizy zawartości obrazu już zarejestrowanego przez kamerę nawet dla kamery, dla której dana reguła analityczna nie była wcześniej aktywna. Usprawnia to znacznie proces poszukiwanie materiału video, gdyż system CCTV w ekspresowym tempie, np. do 300 sekund wyświetli listę znalezionych zdarzeń z wybranego zakresu czasowego odpowiadających wyrysowanej regule, np. pojawienie się osoby w danym wyrysowanym obszarze z możliwością podglądu materiału video skorelowanego ze zdarzeniem z listy spełniających warunek zdarzeń. Powoduje to, iż wyszukanie poszukiwanego zdarzenia nie wymaga ręcznego, czasochłonnego przeszukiwania rejestrowanego materiału video,
- zapisywać meta dane w bazie danych zapewniająca szybkie wyszukiwanie archiwizowanych zdarzeń z wykorzystaniem do tego celu wielu kryteriów (np. egzekucja makra, wskazanie regionu obrazu, zmiana kąta obserwacji kamery, skorelowany indywidualnie tekst, tablice rejestracyjne, twarze, zdefiniowane reguły ruchu) definiowalnych dla wybranych zasobów we wskazanym okresie czasu.

Dla każdego punktu kamerowego możliwe będzie zaimplementowanie algorytmu inteligentnej analizy obrazu bazując na licencjach serwera dającej tym samym możliwość migracji wybranej funkcji wg harmonogramu. Dla wybranego punktu kamerowego możliwa będzie implementacja jednego, dwóch lub wszystkich algorytmów jednocześnie. W zaprojektowanym systemie dostępne są poniższe algorytmy:

- rozpoznawanie tablic rejestracyjnych - algorytm skanuje tablice rejestracyjne wprost z bieżącego strumienia wideo i klasyfikuje znalezioną tablicę przypisując ją do kraju, w którym pojazd jest zarejestrowany. Znalezione tablice mogą być porównywane z, tzw. czarną i białą listą dostępową w wyniku czego generowane są zdarzenia z automatycznym przypisaniem reguły odpowiednich makr np. moduł I/O aktywuje otwarcie szlabanu po wykryciu przez system obecności pojazdu uprawnionego do wjazdu na teren chronionego obiektu. Aktywacja profilu wykrywającego pojazdy opuszczające parking w zdefiniowanym okresie czasu pozwala na wspomaganie procesu zarządzania wolnymi miejscami. W celu minimalizacji ilości fałszywych danych system zapewnia dedykowane wzorce tablic dla min. 120 różnych państw zamiast wykorzystywania generycznego algorytmu skanującego dowolny ciąg znaków. Zwiększenie skuteczności rozpoznania tablic w przypadku zastosowania niezgodnych z zaleceniami kątów ustawieni kamer do płaszczyzny tablicy rejestracyjnej musi być zapewnione przez moduł korekty geometrycznej sceny, który umożliwia dynamiczne zmiany ustawień z poziomu oprogramowania.

Cechy analizy tablic rejestracyjnych:.

- Skuteczność rozpoznania > 98% w systemach parkingowych,
- Programowa korekta geometryczna dla scenariuszy nieoptymalnego kąta montażu kamer,
- Analiza dedykowana do rozwiązań stacjonarnych, parkingowych,
- Eksport/import danych do szeregu typu plików w tym min. CSV, przez zapytania SQL,
- Szablony tablic dla ponad 120 krajów w tym min. Europa, USA, Azja,
- Autoryzacja dostępu na bazie harmonogramów w korelacji z białymi i czarnymi listami dostępu,
- Korelacje rozpoznania tablic (specyficznej tablicy lub grupy tablic) z dowolną akcją, obsługiwaną przez system makr, min.:otwarcie bram, szlabanów, alarmowanie operatora przez przełączenie widoku, wysłanie maila ze zdjęciem, realizacja odpowiedniej sekwencji procedury polityki bezpieczeństwa,
- Zapis danych w bazie danych SQL oraz materiału video i zdjęć MJPEG rozpoznanych pojazdów tablic na podstawie kryterium czasowego i lokalizacji.
- Przekazywanie danych o rozpoznanych tablic dla systemów integrujących w tym min. do systemów zarządzanie bezpieczeństwem systemu SMS

(wielostopniowa weryfikacja dostępu do obiektu w scenariuszu lokalnym i scentralizowannym), systemów parkingowych, itd.
- Łatwość filtrowania zdarzeń dla konkretnej tablicy, grupy tablic.

- rozpoznawanie twarzy - algorytm wyodrębnia z bieżącego obrazu wideo twarze obserwowanych osób przekształcając je do postaci tzw. meta danych. Analizie podlegają punkty nanoszone na brwi, oczy, nos oraz usta. Każda rozpoznana twarz jest porównywana ze wzorcem przechowywanym w bazie danych i na tej podstawie automatycznie klasyfikowana do tzw. czarnej lub białej listy ściśle powiązanej z uprawnieniami dostępu do zasobów obiektu osób, których twarz podlega analizie. Na podstawie wyników tejże analizy, system aktywuje odpowiednią regułę makr. Aktywacja dedykowanego profilu pozwala na weryfikowanie obecności osób we wskazanym miejscu obiektu z podaniem okresu czasu,

- rozpoznawanie reguł ruchu - predefiniowane reguły ruchu izolują i klasyfikują obiekty wprost z bieżącego strumienia wideo. Aktywacja zdarzenia następuje automatycznie w przypadku naruszenia zdefiniowanej reguły. Funkcja pozwala na definiowanie przekroczenia linii, detekcji pozostawionego lub zabranego przedmiotu, przebywania w wyznaczonej strefie z określeniem dozwolonego okresu czasu. Zdarzenie jest korelowane z aktywacją odpowiedniego makra systemowego wyzwalając lawinowo dalsze, powiązane scenariusze systemowe. Dostępne reguły mogą również służyć do budowania systemu zliczania osób oraz innych statystyk ruchu,

- detekcja twarzy na dowolnej obsługiwanej przez platformę kamerze będzie możliwa bez konieczności wykorzystywania dodatkowych licencji lub wykorzystywania dedykowanych kamer. Funkcja ta zapewni możliwość szybkiej weryfikacji post factum pojawiających się osób w scenie obserwowanej przez dany punkt kamerowy w module wyszukiwania zdarzeń oraz możliwość stworzenia scenariuszy alarmowania operatora o pojawiających się osobach, np. w czasie zakończenia pracy obiektu, itd. w połączeniu z silnikiem makr.

System ma mieć możliwość realizacji wielu kombinacji reakcji na aktywacje dowolnej reguły analityki obrazu wbudowanej w kamerze. Potrzebę implementacji algorytmu w wybranych lokalizacjach należy ustalić z Inwestorem i Użytkownikiem obiektu na etapie realizacji i odbiorów.

System musi zapewniać komunikację programową ze zintegrowanym systemem bezpieczeństwa SMS umożliwiając następujące funkcjonalności:

- aktywację predefiniowanych ustawień kamer obrotowych kamer PTZ w wyniku otrzymania przez system SMS informacji alarmowej z systemu SSWiN, KD lub innych,
- zdalne kontrolowanie funkcji PTZ z poziomu mapy synoptycznej systemu SMS,
- generowanie zdarzeń w bazie danych systemu SMS z przypisaniem powiązanego obrazu,
- import zdarzeń będących wynikiem działania algorytmów analizy obrazu,
- wyświetlanie obrazu z kamer w trybie bieżącego podglądu, np. z poziomu mapy synoptycznej systemu SMS,
- odtwarzanie materiału archiwalnego przypisanego do zdarzeń w systemie SMS.

System musi zapewniać komunikację programową z interkomowym systemem komunikacji gwarantując możliwość realizacji następujących funkcjonalności:

- komunikacja dwukierunkowa pomiędzy serwerami systemu CCTV oraz systemu komunikacji głosowej,
- rejestracja dźwięku z terminali interkomowych zsynchronizowanego z obrazem z niezależnej kamery obsługiwanej przez system CCTV na serwerach systemu CCTV w paśmie nie mniejszym niż 7 kHz oraz metodą kompresji G.722,

- możliwość odsłuchania przeprowadzonej rozmowy interkomowej z materiału archiwalnego lub w czasie trwanie rozmowy z poziomu stacji operatorskiej systemu CCTV,
- przełączanie widoków w trakcie trwania rozmowy prezentujących dzwoniącą osobę,
- kontrola elementów systemu komunikacji głosowej z poziomu widoku systemu CCTV, np. inicjalizowanie połączeń interkomowych, sterowanie przejściami poprzez moduł wejść/wyjść terminali interkomowych.

Założenia dla telewizji „medycznej"

Dla potrzeb Wielkopolskiego Centrum Zdrowia Dziecka w Poznaniu zaprojektowano instalację telewizji obserwacyjnej pacjenta/medycznej. System przeznaczony jest do przekazywania obrazu pacjenta na stanowisko pielęgniarek dyżurnych. Na komputerach roboczych znajdujących się w punktach pielęgniarskich będzie zainstalowana aplikacja kliencka systemu CCTV. Kamery zaprojektowano w strefach pacjenta objętego dozorem wizyjnym oraz salach operacyjnych.

Rozmieszczenie urządzeń przedstawiono na podkładach budowlanych.

Obraz przekazywany z kamer podlega obróbce na dedykowanym wyłącznie pod sieć kamer medycznych– serwerze wizyjnym.

System telewizji medycznej/obserwacyjnej pacjenta zaprojektowano w technologii IP jako wydzielony system rejestracji (i przekazu) obrazu z sal części „medycznej" oraz systemem dozoru obiektu (CCTV). Dzięki technologii IP dostęp do każdej z funkcji systemu jest możliwy **wyłącznie dla uprawnionych osób.** Możliwe jest również określenie na drodze programowej (między innymi) następujących parametrów systemu:

- możliwość zdalnego ustawienia parametrów przekazywanych przez kamerę (kamera włączona/wyłączona, określenie pola przekazu obrazu, pala maskowanego, pola aktywnego i inne),
- tworzenie grup podglądu – przypisanie do stanowiska monitorowania kamer wizyjnych oraz uprawnień do modyfikacji parametrów,
- określenie konfiguracji pracy systemu w zależności od pory dnia, np. w nocy z uwagi na ograniczoną liczebność personelu obrazy z wybranych kamer mogą być przekazywane do jednego (zamiast kilku w dzień) z deklarowanego stanowiska monitoringu wizyjnego
- możliwość zdalnego podglądu obrazów z kamer „on line" (lub zapisu z kamer) poprzez PC włączony w sieć Ethernet/Internet po zalogowaniu do serwera systemu w ramach przyznanych uprawnień.

W salach operacyjnych (do ogólnej obserwacji pomieszczenia) znajdujących się na kondygnacji P02 należy zastosować kamery o parametrach nie gorszych niż:

- Czułość przetwornika kamery: kolor: 0.07 Lux , B/W: 0.007 Lux , 0 lux (IR wł.)
- Funkcje : WDR 120 dB ,Defog , HLC , BLC
- Przetwornik 3 Mpx 1/2.8" Progressive Scan CMOS
- Obiektyw Autofocus 2.8-12 mm
- Rozdzielczość :FullHD @60 kl/s , 2048 x 1536 @ 45 kl/s
- Wbudowany promiennik 40 m
- Zakres temperaturowy pracy :--30 °C – 60 °C (-22 °F – 140 °F)
- Pyło-/wodoodporność IP66
- Wandaloodporność IK10

- Wbudowana analiza obrazu : Detekcja przekroczenia linii, detekcja wtargnięcia, wejście na obszar, wyjście z obszaru , bagaż bez dozoru, usunięcie obiektu , Detekcja twarzy , zliczanie obiektów (liczba obiektów wchodzących i wychodzących jest liczona oraz wyświetlana na ekranie w czasie rzeczywistym).

Pozostałe kamery medyczne/systemu obserwacji pacjenta musza posiadać parametry nie gorsze niż:

- Sensor obrazu przetwornik 1/3" typu CMOS
- Minimalne naświetlenie 0.1 lux kolor, 0.01 lux (cz/b), 0 lux z podświetleniem IR
- Szybkość migawki 1/3 s do 1/10,000 s
- Obiektyw zmiennoogniskowy 2,8 do 12 mm, F1. 4
- Automatyczna przysłona DC
- Tryb dzień/noc filtr IR-cut z możliwością demontażu (ICR)
- Podświetlanie IR 24 el., 850 nm
- Odległość skuteczna podświetlania IR do 30 m
- WDR 120 dB
- Udoskonalenie obrazu BLC/ 3D DNR / ROI
- Balans bieli ręczny, AWB1, AWB2, blokada WB, lampa fluorescencyjna, lampa żarowa, światło ciepłe lub naturalne
- Typ H.264 profil główny
- Ilość klatek
- strumień główny: 32kb/s~16384kb/s
- strumień podrzędny: 32kb/s~8192Mb/s
- Maks. rozdzielczość 2688 x 1520
- Przepływność 2688 x 1520 (20/20 kl./s),
- Zestaw funkcji inteligentnych:
- Wykrycie przekroczenia linii przekroczenie wstępnie określonej linii wirtualnej
- Wykrycie wtargnięcia wtargnięcie na wstępnie określony obszar wirtualny
- Detekcja ruchu - 8 zdefiniowanych przez użytkownika, prostokątnych masek; nastawne

  poziomy wykrycia, czułość oraz interwały czasowe
- Sygnalizacja sabotażu wł./wył./zaprogramowana
- obsługa kart pamięci typu SD/SDHC/SDXC o pojemności maksymalnie 128 GB
- Standardy ONVIF (Profil S, Profil G), PSIA, CGI
- autoryzacja użytkownika, znak wodny, filtrowanie po adresie IP, anonimowy dostęp, strumieniowanie kodowane
- Temperatura robocza -30 C do 60 C
- Wilgotność względna 90% lub mniej (bez skroplenia)
- Klasa szczelności IP66
- Odporność na uderzenia IK10

Dla potrzeb poniższych pomieszczeń zaprojektowano implementację algorytmu rozpoznawania reguł ruchu – przekroczenie linii:

oddział	**nr pom.**	**nazwa pom.**	**nr kamery**
SOR	0.014	WSTĘPNA IT	KM.0.1.1

SOR	0.014	WSTĘPNA IT	KM.0.1.2
SOR	0.044	IZOLATKA	KM.0.1.5
OZ	0.312	POK. 1Ł 7 DS IZOL.	KM.0.2.1
OZ	0.383	POK. 1Ł 61 IZOL.	KM.0.2.2
OZ	0.339	POK. 1Ł 22 DM IZOL.	KM.0.3.9
OZ	0.356	POK. 1Ł 39DM IZOL.	KM.0.3.26
IT	2.131	IZOLATKA	KM.2.1.12

W powyższych kamerach proponuje się realizację detekcji po obrysie łóżka. Należy zachować margines 50cm po bokach w celu uniknięcia fałszywych alarmów.

Potrzebę implementacji algorytmów w innych kamerach należy ustalić z Inwestorem i Użytkownikiem obiektu na etapie realizacji i odbiorów.

Łącznie dla potrzeb „medycznej" CCTV zaprojektowano 161 kamer w tym 5 kamer na salach operacyjnych. Nie projektuje się rejestracji obrazu z tych kamer, jednak Inwestor wymaga zapewnienia takiej możliwości. Każdy z zaprojektowanych serwerów wyposażony jest w dedykowane przez producenta systemu dwa dyski o pojemności 8TB każdy w celu zapisu materiału na żądanie.

Należy zastosować serwery o parametrach technicznych nie gorszych niż:

- System operacyjny 64-bit
- Dysk twardy 64GB SSD
- Konfiguracja Raid: standardowa konfiguracja Raid 5 / poza Raid 1 konfiguracja z dwoma dyskami twardymi
- Pojemność zapisu do 40TB (4x 3,5" dyski twarde)
- Procesor 8M Cache, 3.6 GHz
- Pamięć 16 GB
- Interfejs sieciowy podwójny Gigabit Ethernet RJ-45 (10/100/100 MB/s)
- Wejście wideo VGA
- Diagnostyka funkcjonalność monitorowania i alarmowania o anomaliach on-line urządzeń
- sieciowych (przy wykorzystaniu dedykowanej platformy CCTV)
- Typ obudowy 19- calowa o wysokości 1U do montażu w szafie rackowej
- Temperatura pracy 5° C do 40° C (41°F - 104°F)
- Temperatura przechowywania -40° C do 65° C (-40°F - 149°F)
- Serwery należy doposażyć w dedykowane przez producenta dyski 8TB o parametrach nie gorszych niż:
- Bufor do obsługi 256
- Prędkość obrotowa (RPM) 7200
- Średnia latencji (ms) 4.16
- Interfesj SATA 6Gb/s
- Szybkość transmisji interfejsu (MB/s, max) 600
- Czas wyszukiwania 8.6 ms
- Obciążanie/rozładowywanie cykli (przy 40°C) 600,000

- MTBF (M godz.) 2.5
- AFR 0.44% (2TB,4TB,6TB) / 0.35% (8TB,10TB)
- Ciągłość pracy 24h/ 7
- Typ napędu 3,5 -calowy wewnętrzny dysk twardy
- Temperatura otoczenia podczas pracy od 5° do 60° C
- Wibracje (G RMS, 5 to 500 Hz) 0.67 (XYZ)

Kamery pracujące w systemie telewizji medycznej/obserwacyjnej pacjenta włączone są w wydzieloną sieć LAN. Zasilanie kamer zrealizowano poprzez sieć (PoE). Poszczególne elementy instalacji: zasilacze, przełączniki, panele krosowe zamontowane będą w szafach teleinformatycznych RACK 19" oznaczonych jako security i zlokalizowanych w pomieszczeniach teletechnicznych. Wymagania instalacyjne odnośnie klasy łączy i kategorii urządzeń opisano w projekcie instalacji okablowania strukturalnego. Serwer i przełącznik rdzeniowy sieci telewizji zaprojektowano w szafach w serwerowni. Urządzenia instalacji telewizji zasilane będą z obwodów gwarantowanych UPS (230V/50Hz). Z uwagi na zakładaną możliwość zamiany funkcji transmisji oraz fizycznych przełączeń pomiędzy siecią strukturalną i siecią telewizji, należy po zakończeniu robót montażowych przyprowadzić pomiary parametrów sieci wg PN-EN50346 dla klasy EA kanału transmisji w zakresie okablowania miedzianego oraz OF300 dla okablowania światłowodowego.

4.1.8 System bezpieczeństwa SMS

Ze względu na mnogość wymaganych rozwiązań teletechnicznych na obiekcie proponuje się aby systemy teletechniczne w maksymalny możliwy sposób były ze sobą zintegrowane. Umożliwi to wygospodarowanie miejsca dla potrzeb zarządzania budynkiem oraz usprawni jego eksploatację. Z wyżej opisanych powodów projektuje się zastosowanie Systemu Zarządzania Bezpieczeństwem (SMS).

Założenia ogólne

Systemy bezpieczeństwa zainstalowane w obrębie projektowanego Wielkopolskiego Centrum Zdrowia Dziecka w Poznaniu będą w pełni monitorowane i zarządzane z poziomu centralnej platformy Systemu Zarządzania Bezpieczeństwem (SMS). Poniżej przedstawiono najważniejsze cechy funkcjonalne zaproponowanego rozwiązania.

Do najważniejszych funkcjonalności realizowanych przez platformę SMS można zaliczyć:

- zarządzanie elementami sprzętowymi i logicznymi poszczególnych podsystemów;
- konfiguracja parametrów urządzeń wchodzących w skład poszczególnych podsystemów;
- pełna wizualizacji stanu elementów sprzętowych i logicznymi poszczególnych podsystemów;
- korelacja zdarzeń występujących w kilku podsystemach w oparciu o funkcje logiczne;
- jedna baza danych użytkowników i zdarzeń dla wszystkich podsystemów.

Projektowany system bezpieczeństwa opracowany został w celu zapewnienia bezpieczeństwa osób i mienia znajdujących się na terenie obiektu. Platforma zarządzania SMS będzie realizować wzajemne współdziałanie poniższych podsystemów za pomocą interfejsów programowych:

- Kontroli Dostępu,
- Monitoringu Wizyjnego CCTV,
- Interkomowego,

- Systemu Sygnalizacji Włamania i Napadu,
- Systemu kolejkowego,
- Systemu RCP,
- Systemu windowego,
- Sygnalizacji Pożarowej (wizualizacja).

Dodatkowo system SMS musi umożliwiać integrację systemów zewnętrznych, m.in.:

- Zarządzania kluczami,
- Monitoringu środowiskowego.

Każda z funkcjonalności musi być dostępna zarówno na etapie projektu i wdrażania, jak i ewentualnej rozbudowy działającego systemu. Dodatkowo każdą z funkcjonalności oraz każdy z modułów będzie można płynnie rozbudowywać w przyszłości.

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

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

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

Informacja o błędach w komunikacji jest także odzwierciedlana diodami sygnalizacyjnymi umieszczonymi na sterowniku lokalnym.

Zastosowanie Systemu Zarządzania Bezpieczeństwem (SMS) ma skutkować znaczącym obniżeniem kosztów utrzymania i eksploatacji systemu bezpieczeństwa przez:

- Zautomatyzowanie procesu detekcji sytuacji alarmowej;
- Ograniczenie liczby kadry pracowniczej wewnętrznej lub zewnętrznej odpowiedzialnej za monitorowanie systemów bezpieczeństwa;
- Optymalizację procesu konfiguracji poszczególnych podsystemów przez administratora systemów;
- Ograniczenie kosztów ewentualnych działań serwisowych przez możliwość rekonfiguracji zdalnej.

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

Dane przesyłane w systemach zabezpieczeń są kluczowe dla zachowania bezpieczeństwa. Z tego względu system SMS musi wykorzystywać najwyższej klasy protokoły kryptograficzne.

Komunikacja między serwerem a stacją roboczą (stanowisko wizualizacji, punkt zdalnego zarządzania, terminal modyfikacji parametrów) musi się odbywać przez sieć TCP/IP z wykorzystaniem protokołu SSL, ze 128-bitowym kluczem.

Integracje w ramach SMS

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

System musi umożliwiać horyzontalny podział bazy danych w ramach jednego serwera na kilka odseparowanych od siebie części logicznych. Każdy operator będzie miał dostęp do zdarzeń, mapy synoptycznej i użytkowników tylko w zakresie ograniczonej części chronionego obiektu (np. jednego piętra). Zwiększa to możliwość definiowania odpowiednich uprawnień poszczególnych operatorów. Dodatkowo musi istnieć możliwość sekwencyjnej obsługi systemu, czyli automatycznego przełączania obsługi określonego obszaru między ściśle określonymi operatorami w momencie wylogowania z systemu SMS jednego z operatorów.

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

System musi pozwalać na pisanie procedur programowych pozwalając na reagowanie w zależności od kilu zmiennych (algebra Boole`a dla co najmniej dwóch warunków). Działania mogą dotyczyć zdarzeń występujących w różnych podsystemach.

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

- Raport zdarzeń i częstotliwości występowania zdarzeń;
- Raport listy użytkowników z danymi osobowymi;
- Raport obecności dla danego użytkownika i dla danego obszaru;
- Raport praw dostępu dla użytkownika i czytnika;
- Raport ścieżki użycia karty na obiekcie;
- Raport stanu sterowników i podłączonych do nich urządzeń;
- Raport stanu błędów występujących w systemie.

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

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

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

Kluczowy z punktu widzenia bezpieczeństwa i samej obsługi systemu jest interfejs użytkownika. Platforma musi oferować czytelny i intuicyjny interfejs użytkownika GUI. System musi umożliwiać przypisanie w bazie danych do użytkownika następujących danych:

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

Dodatkowo istnieje możliwość zdefiniowania co najmniej 20 dowolnych pól dodatkowych, których może wymagać Użytkownik. Każdy z użytkowników po zalogowaniu się do systemu może korzystać z interfejsu w wybranym języku: polski, niemiecki, angielski. Język interfejsu musi być przypisany do użytkownika, a nie do urządzenia. System musi umożliwiać definiowanie wymogów odnośnie hasła operatora, m.in. w zakresie ilości wymaganych znaków i typów znaków. Standardowo platforma SMS musi wymagać od operatora wprowadzenia hasła złożonego co najmniej z 6 znaków, z których przynajmniej jeden to cyfra, a inny to wielka litera.

Zarządzanie uprawnieniami i personalizacja stanowiska pracy musi być przypisywana poszczególnym profilom użytkownika, a nie konkretnym stanowiskom operatorskim. Musi istnieć możliwość przypisywania dostępu do poszczególnych modułów, map synoptycznych i innych elementów graficznego interfejsu użytkownika odpowiednim operatorom w zależności od ich uprawnień. Platforma SMS musi umożliwiać definiowanie typu działań, które operator może realizować na poszczególnych danych systemowych (m.in. podgląd, edycja, usunięcie). Po wprowadzeniu zmian konfiguracyjnych system nie może wymagać resetowania poszczególnych stacji operatorskich, wystarczające jest zapisanie zmian na serwerze głównym.

Funkcjonalności międzysystemowe

Wymaga się aby Platforma SMS umożliwiała realizację następujących funkcjonalności międzysystemowych:

Podsystem monitoringu wizyjnego

- Wywołanie okna widoku kamery CCTV w sytuacjach alarmowych wywołanych przez system KD, SSWiN lub kamery systemu interkomowego (obraz wideo wspiera procesy decyzyjne w systemie) w platformie SMS.
- Rozpoczęcie zapisu materiału wideo z kamer systemu CCTV, w momencie wystąpienia określonych zdarzeń w pozostałych systemach (KD, SSWiN, SSP, Interkomowym, RCP). Zapisany materiał jest przypisany do konkretnego zdarzenia
- W przyszłości opcjonalną Integrację funkcji analitycznych rozpoznawania numerów rejestracyjnych aut realizowaną przez system CCTV, czy rozpoznawania twarzy z systemem kontroli dostępu. Numer rejestracyjny lub wzór twarzy pełni rolę karty dostępowej w systemie kontroli dostępu.
- Przesłanie informacji o przekroczeniu wirtualnej linii i detekcji ruchu do systemu SMS oraz rozpoczęcie określonej procedury alarmowej.

Prezentację bezpośrednio na mapie synoptycznej obrazu z kamer. Dodatkowo możliwość wysterowania kamer PTZ oraz realizację „Presetu” bezpośrednio z mapy synoptycznej

Podsystem interkomowy

- Wywoływanie połączenia interkomowego z poziomu platformy SMS oraz prezentacja obrazu z kamery, przypisanej do danego interkomu. Dodatkowo w momencie

wystąpienia połączenia przychodzącego, operator widzi na mapie synoptycznej z jakiego interkomu nawiązywana jest rozmowa.

- Generowanie automatycznych komunikatów głosowych z systemu interkomowego, w sytuacjach zagrożenia (komunikaty generowane automatycznie, w określonych sytuacjach oraz uruchamiane ręcznie przez osoby nadzorujące system).
- Automatyczne rozpoczęcie rozmowy interkomowej w momencie wystąpienia odpowiednich zdarzeń w pozostałych systemach.
- Prezentacja informacji o interkomach bezpośrednio w platformie SMS. Prezentowane są informacje o statusie każdego z interkomów (prowadzi rozmowę, oczekuje itp.).

Podsystem sygnalizacji pożarowy

- Przesyłanie informacji o zdarzeniach alarmowych z centrali SSP do systemu SMS i rozróżnienie rodzaju alarmu, np. alarm pożarowy czujki, alarm pożarowy strefy, alarm tampera, brak połączenia między centralą a serwerem itp.
- Definiowanie dowolnych procedur działania alarmowego w platformie SMS i kroków, które operator systemu musi wykonać (np. wywołanie komunikatu z systemu interkomowego itp.).
- Wizualizacja na mapie synoptycznej stanu poszczególnych detektorów i/lub stref SSP; prezentacja stanu stref może być przedstawiona jako dynamiczna ikona umieszczona w danym pomieszczeniu lub jako pozycja w tabeli na dedykowanej mapie synoptycznej.

Podsystem zarządzami windami

- Aktywacja przycisków wyboru pięter w oparciu o uprawnienia użytkowników, realizowana za pomocą czytników kontroli dostępu umieszczonych w windach.
- Po przyłożeniu karty do czytnika kontroli dostępu, przekazywanie informacji o domyślnym numerze piętra odpowiednim dla danego użytkownika z platformy SMS do systemu zarządzania windami.
- Przesyłanie informacji o zdarzeniach alarmowych z podsystemu zarządzania windami do platformy SMS.
- Definiowanie dowolnych procedur działania alarmowego w platformie SMS i kroków, które operator systemu musi wykonać.

Intergracja Systemu Kontroli Dostępu z systemem Rejestru Czasu Pracy

- System KD odczytuje odbicia na wybranych czytnika wejściowych i wyjściowych (terminal RCP z możliwością rozróżnienia początku, końca pracy oraz wyjścia służbowe/prywatne)
- Dane z terminala wysyłane są do systemy RCP powiązanego z systemem kadrowo płacowym w formacie xml.. Dane o pracownikach będą importowane do systemu KD z pliku xml z systemu kadrowo płacowego.

Integracja z systemem kolejkowym

- System KD będzie wyposażony w czytniki kart z zintegrowanymi czytnikami kodów QR, które będą przeznaczone dla uzyskania informacji z systemu kolejkowego.
- W systemie KD zostanie na stałe przydzielone numery kart do systemu kolejkowego.
- Dla każdej kolejki zdefiniowane zostania kody 2D/QR drukowane na biletach. Czytniki SKD będą miały zaprogramowaną listę kodów, które będą umożliwiały przejście. Wartości kodów będą stałe w czasie i dla każdego pacjenta.

Protokoły komunikacyjne

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

Komunikacja między serwerem centralnym a sterownikiem kontroli dostępu musi się odbywać w oparciu o protokół TCP/IP. Przesyłane dane muszą być szyfrowane za pomocą standardu AES-CBC (256 bit). Dla każdej sesji musi być generowany nowy klucz, aby zapobiec powtórzeń kluczy. Klucze muszą być zapisane w pliku XML, który musi być zabezpieczony za pomocą szyfrowania AES-256.

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

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

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

Serwer

Jednostką główną systemu musi być serwer w standardzie RACK, który ma zostać zamontowany w szafie serwerowej. System ma być oparty o stabilniejsze niż OS Windows środowisko UNIX. System musi instalować tylko ten fragment jądra UNIX, który jest wymagany do realizacji zadań SMS, aby zminimalizować ryzyko włamania się do systemu użytkowników zewnętrznych. Jednostką główną musi być serwer o parametrach nie gorszych niż:

- Serwer 19”, redundantny zasilacz, 2x USB, DVD-ROM
- Montaż 1U , Głębokość max: 635mm
- Processor: Intel Xeon E5-2420 Processor (1,9GHz, 15M Cache)
- RAM: 12GB (3x 4GB)
- Ethernet: 4x Gigabit Ethernet port
- Dysk HDD: 2x 300GB, RAID 1
- Zainstalowany system Ubuntu

Elementami wykonawczymi platformy SMS muszą być inteligentne sterowniki sieciowe pozwalające na podłączenie elementów wykonawczych systemu Kontroli Dostępu, SSWiN i elementów systemu parkingowego. W przypadku zerwania łączności kontrolera sieciowego z serwerem, musi on nadal zarządzać elementami do niego podłączonymi. Dodatkowo musi zarejestrować w pamięci, co najmniej 20000 zdarzeń. Po ponownym podłączeniu go do serwera musi nastąpić automatyczna, wzajemna synchronizacja.

Wizualizacja (mapa synoptyczna)

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

- System Kontroli dostępu – wizualizacja stanów czytnika, kontaktronu, elektrorygla i wszystkich elementów dodatkowych. Po kliknięciu ikony czytnika powinna zostać wyjustowana lista wyboru trybów pracy czytnika (m.in. stan otwarty, stan normalny, stan z potwierdzeniem operatora).

- System Sygnalizacji Włamania i Napadu – wizualizacja stanów poszczególnych elementów detekcyjnych (np. czujek ruchu PIR). Zazbrajanie i rozbrajanie poszczególnych stref SSWiN.
- System Monitoringu wizyjnego – kliknięcie ikony kamery ma spowodować wyświetlenie obrazu z danej kamery. Możliwość umiejscowienia na mapie synoptycznej przycisków, wymuszających obrót kamery PTZ w konkretne miejsce (preset).
- System Interkomowy – kliknięcie ikony interkomu ma skutkować wywołaniem połączenia z danym interkomem oraz prezentację obrazu z kamery skierowanej na interkom.

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

- Listę osób znajdujących się w danej strefie kontroli dostępu;
- Wykresy zawierające liczby osób przechodzących przez dane przejście;
- Listę stref SSWiN z informacją o ich stanie, umożliwiającą zazbrajanie i rozbrajanie poszczególnych stref;
- Skróty do konkretnych pozycji w menu, szczególnie często używanych przez operatora;
- Listę urządzeń z informacją o ich stanie połączenia z serwerem.

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

4.1.9 Instalacja przyzywowa

Informacje ogólne

Normy

Zaprojektowano system przyzywowy w technologii IP. Wyposażenie poszczególnych pomieszczeń w elementy systemu uzgodniono z Inwestorem na etapie projektu. Rozmieszczenie elementów pokazano w części rysunkowej.

Zaprojektowany system przyzywowy spełnia w pełnym zakresie normy i przepisy:

- DIN-VDE 0834 – instalacje przyzywowe w szpitalach, domach opieki i tym podobnych instytucjach,
- DIN-VDE 0834 / część 1 – wymogi dla urządzeń, ich produkcji i pracy w obiektach,
- DIN-VDE 0834 / część 2 – kompatybilność elektromagnetyczna i wymogi środowiskowe,
- EN60601 – Medyczne urządzenia elektryczne – Część 1: Wymagania ogólne dotyczące bezpieczeństwa podstawowego oraz funkcjonowania zasadniczego,
- EN60950 – Urządzenia techniki informatycznej – Bezpieczeństwo – Część 1: Wymagania podstawowe,
- EN50178 – Urządzenia elektroniczne do stosowania w instalacjach dużej mocy,
- EN50173-1 - Technika informatyczna - Systemy okablowania strukturalnego - Część 1: Wymagania ogólne.

Wymagania dla systemu

- Instalacja przyzywowa powinna zostać wykonana na odrębnej sieci strukturalnej.
- Szybkość transmisji danych w sieci przeznaczonej dla systemu powinna wynosić 100Mb/s.
- Okablowanie strukturalne musi być sprawdzone i przetestowane zgodnie z normą EN 50173-1 klasa D dla kategorii oprzewodowania 5e (kat.5e).
- Niskie napięcie nie może być wykorzystywane równolegle do zasilania innych urządzeń lub sprzętu, za wyjątkiem przekaźnika impulsowego oraz złącz w celu bezpiecznego odłączenia.
- Dla zasilania systemu z ogólnej sieci energii elektrycznej należy stworzyć własne elektryczne obwody zasilające z bezpiecznikami. Przyłączanie innych urządzeń do tych obwodów elektrycznych nie jest dopuszczalne.
- W przypadku zakłóceń ogólnego zasilania w energię, system musi zostać zasilony z awaryjnego źródła prądu w celu bezpieczeństwa. Przejęcie zasilania musi nastąpić najdalej po 15 s od przerwy w dostawie energii i podtrzymać pracę przez minimum 1h. Przerwa w dostawie energii musi zostać zgłoszona.
- Końcówki przewodów należy oznaczyć w sposób wyraźny i trwały.
- W celu ochrony przed niebezpiecznymi porażeniami w pomieszczeniach grup użytkowania 1 i 2 należy stosować wymagane dla tych pomieszczeń środki ochrony.
- Wszystkie przewody ochronne (PE) połączone z systemem muszą być podłączone do tej samej głównej szyny w celu wyrównania potencjałów. Jeżeli nie jest to możliwe w przypadku urządzeń rozległych, wówczas w celu spełnienia tego wymogu muszą zostać rozdzielone obwody elektryczne systemu na wiele podobwodów, które są od siebie oddzielone galwanicznie.
- Urządzenia sterujące, urządzenia zasilające i inne części systemu nie posiadające funkcji obsługi lub sygnału mogą zostać umieszczone wyłącznie w suchych pomieszczeniach, jednak nie w pokojach pacjentów. Muszą one w każdej chwili być dostępne (wejście rewizyjne o szerokości minimum 60cm). Odprowadzanie ciepła nie może zostać zakłócone. W przypadku wmontowania do szaf przyłączowych lub tym podobnych ciepło musi zostać ewentualnie odprowadzone za pomocą wentylacji mechanicznej.
- Aby zagwarantować prawidłowe funkcjonowanie urządzenia w pełnym zakresie, koniecznie zaleca się zamknięcie pętli oprze wodowania magistrali wejścia/wyjścia (IO BUS).

Wymagania dla okablowania

- Maksymalna wymagana szerokość pasma wewnątrz 100Mb (od switch i downlink)
- Wymagana szerokość pasma na zewnątrz do Centrum Zarządzania 1GB
- Zachowanych promień gięcia kabla transmisji danych, montaż podtynkowy lub w płycie kartonowo gipsowej
- Średnica zewnętrzna żyłki maksymalnie 1mm (wliczając osłonę)
- Wtyczka RJ45 dla drutu jednolitego
- Każda sieć LAN zainstalowana dla systemu przezywowego podlega normie kontroli EN50173-1 i musi być sprawdzona i odebrana.

Zasilanie

Z rozdzielnicy dedykowanej dla obwodów teletechnicznych należy wyprowadzić kabel zasilający do zasilacza znajdującego się w pomieszczeniu technicznym danego piętra. Poprzez zasilacz należy doprowadzić napięcie +24V DC do systemowego przełącznika. Oprzewodowanie YLY 2x2,5mm2. W przypadku zasilania kilku przełączników z należy je łączyć ze sobą szeregowo

zgodnie ze schematem ideowym dla danego poziomu. Przełączniki zlokalizowane są w szafach RACK w danym pomieszczeniu teletechnicznym.

Przełącznik systemowy

Switch systemowy spełnia zadania lokalnego węzła komunikacyjnego. Łączy on wszystkie przyłączone urządzenia sprzętowe za pomocą sieci. Przyciski przywoławcze, zaznaczenia obecności/kasujące itd. są przyłączone do switch'a systemowego przez magistralę wej./wyj. (I/O BUS) do sieci. Switch systemowy udostępnia osiem przyłączeń 100Mb LAN (port 1 – port 8). Interfejsy przewidziane są do przyłączenia do nadrzędnego switch'a, połączenie z kolejnym oraz do przyłączenia urządzeń takich jak terminal pacjenta, terminal oddziałowy, terminal komunikacyjny. Przełącznik należy zamontować w szafie RACK. Bezwzględnie należy zachować maksymalną odległość wynoszącą 60m od switch'a do najdalej zamontowanego elementu. Ciepło od urządzeń należy odprowadzić za pomocą wentylacji mechanicznej.

Okablowanie

Oprzewodowanie od zasilacza +24 V do przełącznika systemowego oraz od przełącznika do przełącznika należy wykonać przewodem YLY 2x2,5mm2.

Oprzewodowanie z przełącznika systemowego do urządzeń systemu wykorzystujących magistralę we/wyj. (I/O BUS) należy wykonać kablem kat. 5e UTP 4x2x0,5.

Oprzewodowanie z przełącznika systemowego do urządzeń systemu wykorzystujących port 1 – port 8, należy wykonać kablem kat. 5e F-UTP 4x2x0,5.

Obliczanie długości przewodów magistrali IO

Obliczenie maksymalnej długości magistrali w układzie pętli w zależności od ilości elementów i poboru prądu wykonane zostało dla dwóch pętli najdłuższej oraz najbardziej obciążonej. Poniżej przedstawiono wyniki obliczeń.

I/O - Bus	Ilośc elementów	Prąd	Maksymalna długość pętli
-	[szt.]	[A]	[m]
SW – 0.6	24	0,32	250,12
SW – 2.5	8	0,37	316,79

Rozmieszczenie urządzeń i ich funkcja

Przy montażu urządzeń należy przestrzegać postanowień normatywnych w celu ochrony przed niebezpiecznymi porażeniami w pomieszczeniach grup użytkowania 1 i 2. W tym celu należy stosować wymagane dla tych pomieszczeń środki ochronne. Wszystkie przewody ochronne (PE) połączone z systemem muszą być podłączone do tej samej szyny w celu wyrównania potencjałów. Urządzenia sterujące, zasilające i inne części systemu nie posiadające funkcji obsługi lub sygnału mogą zostać umieszczone wyłącznie w suchych pomieszczeniach, jednak nie w pokojach pacjentów. Muszą one być dostępne w każdej chwili.

<u>Pokojowa lampka sygnalizacyjna</u>

Pokojowa lampka sygnalizacyjna służy do optycznego wskazywania w odpowiednim kolorze przywołań, obecności oraz przekierowanych obecności, zgodnie z normą VDE0834. Obudowa z tworzywa sztucznego z płytką kontrolera. Składa się z 4 komór oświetleniowych z reflektorami świetlnymi dla jednolitego sygnału świetlnego:

- 4 komór z reflektorami dla jednolitego sygnału świetlnego,
- 1 komory wyposażonej w 3 świecące jaskrawoczerwone diody LED,
- 1 komory wyposażonej w 3 świecące jaskrawobiałe diody LED,
- 1 komory wyposażonej w 3 świecące jaskrawozielone diody LED,

- 1 komory wyposażonej w 3 świecące jaskrawoniebieskie diody LED,
- każda komora oświetleniowa spełnia wymagania natężenia światła zgodnie z VDE0834.
- Funkcjonalność:
- optyczne wskazywania przywołań, obecności personelu i przekierowań personelu zgodnie z normą VDE0834.
- kolor zielony –obecność pielęgniarki w pomieszczeniu,
- kolor czerwony ciągły – przywołanie z pomieszczenia uruchomione przez osobę potrzebującą pomocy w celu przywołania pielęgniarki,
- kolor czerwony ciągły i biały – przywołanie z pomieszczenia WC uruchomione przez osobę potrzebującą pomocy w celu przywołania pielęgniarki,
- kolor czerwony migający i zielony ciągły- przywołanie z pokoju uruchomione przez personel w celu przywołania kolejnej osoby z personelu pielęgniarskiego,
- kolor niebieski ciągły – obecność lekarza w pomieszczeniu,
- kolor niebieski migający i zielony ciągły- przywołanie z pokoju uruchomione przez personel w celu przywołania lekarza.

Montaż:

Lampki sygnalizacyjne zostały rozmieszczone w sposób jednoznaczny przy drzwiach od pomieszczeń objętych systemem tak, aby były widoczne dla personelu obsługującego. Wysokość montażu lampek sygnalizacyjnych 1,5m -2,2m nad poziomem podłogi. Lampki montowane nad drzwiami należy montować 20cm nad górną krawędzią drzwi. Lampki wyniesione z wnęk należy montować na tej samej wysokości jak pozostałe zachowując wysokość montażu dla lampek pokojowych. Należy zachować odstęp 15cm od krawędzi ściany oraz 10cm od bocznej krawędzi drzwi. Lampki grupowe montować w odległości 17cm od osi modułów.

Terminal komunikacyjny z wyświetlaczem

Do montażu w pokojach diagnostyki, zabiegowych, lekarzy, pokojach pielęgniarek, w salach podwyższonego nadzoru, w salach segregacji medycznej, salach obserwacyjnych w których personel będzie mógł odbierać wszystkie przywołania zaistniałe na oddziale.

Cechy:

- w pełni graficzny wyświetlacz o rozdzielczości minimum 128 x 64 pikseli,
- elektroniczny buczek dla funkcji akustycznego przekierowania przywołań,
- klawiaturę membranową przeznaczoną do obsługi, na którą składają się:
- przycisk przywoławczy (czerwony) z podświetleniem i diodą LED potwierdzającą,
- przycisk przywołania lekarza (niebieski) z podświetleniem i diodą LED potwierdzającą,
- przycisk zaznaczenia obecności (zielony) z kontrolną diodą LED,
- przycisk zaznaczenia obecności (niebieski) z kontrolną diodą LED,
- przyciski funkcyjne dla regulacji jasności i kontrastu wyświetlacza oraz głośności buczka.

Funkcjonalność:

- przywołanie personelu pielęgniarskiego (przywołanie normalne),
- przywołanie kolejnej osoby personelu pielęgniarskiego (przywołanie o wyższym priorytecie),
- przywołanie lekarza (przywołanie o najwyższym priorytecie),
- odbieranie przywołań przez personel pielęgniarski - po zaznaczeniu obecności,

- odbieranie przywołań przez personel pielęgniarski - po zaznaczeniu obecności,
- pokazywanie szczegółowych informacji tekstowych o przychodzących przywołaniach na wyświetlaczu graficznym,
- kasowanie przywołań.
- Urządzenie to pokryte zostało powłoką antybakteryjną, która redukuje rozprzestrzenianie się bakterii, wirusów, grzybów. Tym samym ułatwia ona znacznie przeprowadzenie szybkiej i skutecznej dezynfekcji.

Montaż:

Terminale w salach chorych itd. powinny być umieszczone na wysokości na wysokości głowy oraz w polu widzenia wszystkich użytkowników pomieszczenia, a także gwarantować możliwość szybkiego dostępu poprzez personel medyczny przy wchodzeniu i opuszczaniu pomieszczenia. Terminale komunikacyjne montować należy na wysokości 1,5m – 1,7m.
W przypadku montażu przy drzwiach bocznych czy krawędzi ściany należy zachować odległość 15cm. Terminal komunikacyjny umieszczać w wolnej ściance obok drzwi, w salach chorych z łazienkami na ścianie zwróconej w kierunku łóżek. Jeśli brak jest możliwości montażu jak wskazano wcześniej wówczas terminal montować na ścianie przeciwległej do łóżek.

Terminal komunikacyjny bez wyświetlacza

Do montażu w pomieszczeniach WC na oddziale.

Cechy:

- elektroniczny buczek dla funkcji akustycznego przekierowania przywołań,
- klawiaturę membranową przeznaczoną do obsługi, na którą składają się:
- przycisk przywoławczy (czerwony) z podświetleniem i diodą LED potwierdzającą,
- przycisk przywołania lekarza (niebieski) z podświetleniem i diodą LED potwierdzającą,
- przycisk zaznaczenia obecności (zielony) z kontrolną diodą LED,
- przycisk zaznaczenia obecności (niebieski) z kontrolną diodą LED,
- 3 przyciski funkcyjne dla regulacji jasności i kontrastu wyświetlacza oraz głośności buczka.

Funkcjonalność:

- przywołanie personelu pielęgniarskiego (przywołanie normalne),
- przywołanie kolejnej osoby personelu pielęgniarskiego (przywołanie o wyższym priorytecie),
- przywołanie lekarza (przywołanie o najwyższym priorytecie),
- odbieranie przywołań przez personel pielęgniarski - po zaznaczeniu obecności,
- odbieranie przywołań przez personel pielęgniarski - po zaznaczeniu obecności,
- kasowanie przywołań.

Przycisk z mechanizmem pociągowym

Miejsce montażu (zgodne z projektem):

- w łazienkach / WC lub w innym ważnym pomieszczeniu do przywołania pielęgniarki.

Cechy:

- mikroprzełącznik z 2-metrową linką pociągową z karabinkiem, zakończona uchwytem
  z symbolem pielęgniarki (ze względów higienicznych uchwyt jest wymieniany w prosty sposób),

- linka wraz z systemem mocować musi ulec zerwaniu przy maks. sile zrywającej 120N odpowiadającej wadze ok. 12 kg),
- dioda LED podświetlająca/potwierdzająca.

Funkcjonalność:

- przywołanie personelu pielęgniarskiego (przywołanie normalne),
- przywołanie kolejnej osoby personelu pielęgniarskiego (przywołanie o wyższym priorytecie).

Montaż:

Przyciski przywoławcze w WC i łazienkach muszą być dobrze dostępne. W łazienkach uchwyt linki pociągowej powinien znajdować się w bezpośrednim zasięgu ręki kąpiącej się osoby. Montaż przycisku do pociągania możliwy jest na ścianie obok wanny powyżej 20cm od główki prysznica. W przypadku wanny stojącej na wolnej przestrzeni montaż wykonać na suficie. W przypadku znajdującego się obok WC przycisk może być jeden wspólny ale dostępny z obu miejsc. Ze względu na wilgoć w pomieszczeniach sanitarnych należy zachować strefy ochrony 0, 1, 2.

Strefa ochronna 0:

Strefa 0 definiuje wnętrze wanny lub basenu natryskowego. W przypadku pryszniców bez wanny (prysznice na poziomie ziemi) nie istnieje strefa 0. Obowiązuje wówczas promień 120cm wokół główki prysznica jako strefa 1.

Strefa ochronna 1:

Strefa 1 rozciąga się ponad strefą ochronną 0 aż do wysokości minimum 2,25m, jeśli przyłączenie wody znajduje się wyżej (np. w przypadku prysznica), wówczas do tej wysokości, ponad podłogą i obowiązuje dla powierzchni ponad wanną lub prysznicem lub obszaru poniżej wanny lub wanny z prysznicem aż do powierzchni instalacji.

Strefa ochronna 2:

Strefa 2 obowiązuje dla obszaru o szerokości 60 cm od wanny lub prysznica, będącego w zasięgu ręki. Po obu stronach ściany do wysokości 2,25m od poziomu podłogi. Przy wejściach od kabin prysznicowych jest to okrąg z środkiem wyznaczonym przez ścianę kabiny prysznicowej. Obowiązują tutaj wymagania strefy 1. Nie wolno montować gniazd, łączników oświetleniowych, puszek łączeniowych itp.

<u>Przycisk przywoławczy</u>

Miejsce montażu w uchwycie przy łóżku pacjenta.

Cechy:

- przycisk przywoławczy z symbolem pielęgniarki na stronie czołowej z podświetleniem
  i diodą potwierdzającą, służący do przywołania personelu pielęgniarskiego (przywołania normalne), jeżeli w pomieszczeniu przebywa personel pielęgniarski wówczas za pomocą przycisku można wyzwolić przywołanie kolejnej osoby z personelu pielęgniarskiego (przywołanie o wyższym priorytecie)
- kabel przyłączeniowy o długości 2,8m z samoczynnie wypinającą się wtyczką chroniącą przed przerwaniem lub wyrwaniem.

Funkcjonalność:

- przywołanie personelu pielęgniarskiego (przywołanie normalne),
- przywołanie kolejnej osoby personelu pielęgniarskiego (przywołanie o wyższym priorytecie).

Przycisk podłączany jest do modułu gniazdkowego typ 2.

Przycisk kasujący

Do montażu w pojedynczej puszce instalacyjnej, składa się z ramki montażowej z płytką drukowaną, na której znajdują się elementy elektroniki funkcyjnej i dozorujące linię przywołania, klawiatura foliowa, jak również:

- 1 przycisk kasujący (zielony) z kontrolną diodą LED,
- 2 gniazda RJ45 dla przyłączenia magistrali danych,
- w komplecie ramka montażowa dla zatrzaskowego mocowania na puszce instalacyjnej.

Przycisk kasujący montować 10cm od krawędzi drzwi na wysokości 0,7m-1,5m.

Moduł gniazdkowy typ 1

Moduł gniazdkowy umiejscowiony 0,5m od podłogi pod biurkiem, na którym będzie znajdował się terminal oddziałowy (montaż nabiurkowy). Przy montażu wszystkich elementów i urządzeń należy zwrócić szczególną uwagę na dobry dostęp do prowadzenia prac montażowych i serwisowych.

Moduł gniazdkowy typ 2

Miejsce montażu (zgodne z projektem)

- sala chorych przy łóżku pacjenta

Cechy:

- wyposażony w mechanizm automatycznego wypięcia się wtyczki, chroniącego wtyczkę przed zniszczeniem,
- gniazdo diagnostyczne umożliwiające wedle potrzeby podłaczenie: urządzenia medyczne posiadające alarmowy zestyk bezpotencjałowy, tj inkubatory, pompy infuzyjne itp.

Funkcjonalność:

- podłączenie przycisku „gruszkowego”

W panelu medycznym należy przewidzieć miejsce na moduł gniazdkowy i przekaźnik sterowania oświetleniem. Wysokość gniazda winna być na wysokości 1,6m – 1,8m nad poziomem podłogi.

Moduł gniazdkowy typ 3

Miejsce montażu (zgodne z projektem)

Cechy:

- przycisk przywoławczy z symbolem pielęgniarki na stronie czołowej z podświetleniem
  i diodą potwierdzającą, służący do przywołania personelu pielęgniarskiego (przywołania normalne), jeżeli w pomieszczeniu przebywa personel pielęgniarski wówczas za pomocą przycisku można wyzwolić przywołanie kolejnej osoby z personelu pielęgniarskiego (przywołanie o wyższym priorytecie)
- przycisk kasujący
- wyposażony w mechanizm automatycznego wypięcia się wtyczki, chroniącego wtyczkę przed zniszczeniem.
- gniazdo diagnostyczne umożliwiające wedle potrzeby podłaczenie: urządzenia medyczne posiadające alarmowy zestyk bezpotencjałowy, tj inkubatory, pompy infuzyjne itp.

Funkcjonalność:

- podłączenie przycisku gruszkowego
- przywołanie personelu pielęgniarskiego (przywołanie normalne),

- przywołanie kolejnej osoby personelu pielęgniarskiego (przywołanie o wyższym priorytecie),
- kasowanie przywołań.

Terminal oddziałowy

Przeznaczony jest do zastosowań w oddziałowych pomieszczeniach w punktach pielęgniarskich.

Cechy:

- kolorowy wyświetlacz ciekłokrystaliczny 5,6”
- 12 interaktywnych przycisków funkcyjnych.
- intuicyjna obsługa (wyświetlacza) pozwala na szybką reakcję personelu nawet w stresujących sytuacjach.

Funkcjonalność:

- odbieranie przywołań na linii personel ←→ pacjent, personel ←→ personel,
- zmienianie (podnoszenie/obniżanie) priorytetu przywołania z łóżka pacjenta,
- przywoływanie personelu pielęgniarskiego,
- przywoływanie personelu lekarskiego,
- łączenie oddziałów w celu przekierowywania przywołań,
- wyświetlanie informacje o uszkodzeniach urządzeń w systemie z dokładnością minimum co do pomieszczenia (system automatycznie kontroluje stan pracy urządzeń).

Kabel przyłączeniowy (2,8 m) zakończony wtyczką RJ45 w wykonaniu odpornym na wyrwanie.

Terminale oddziałowe winny być przyłączane do gniazdka podłączeniowego umiejscowionego 0,5m od podłogi pod biurkiem, na którym będzie znajdował się terminal (montaż nabiurkowy). Przy montażu wszystkich elementów i urządzeń należy zwrócić szczególną uwagę na dobry dostęp do prowadzenia prac montażowych i serwisowych.

Prowadzenie instalacji

Przewody obwodów elektrycznych systemu nie mogą być prowadzone we wspólnych kablach wraz z przewodami urządzenia elektroenergetycznego lub innymi instalacjami przewodzącymi niebezpieczne napięcie. Przewody obwodów elektrycznych nie mogą być prowadzone w tych samych rurkach lub kanałach instalacyjnych, co przewody instalacji elektroenergetycznych lub innych instalacji przewodzących niebezpieczne napięcie. Przewody systemu i urządzenia elektroenergetycznego należy układać z zachowaniem minimalnej odległości 30cm. W przypadku krótkich odcinków odstęp można zmniejszyć do 10cm. Zaciski dla systemu i urządzeń muszą w sposób wyraźny różnić się od siebie np. formą / kolorem. Same napisy nie stanowią wystarczającej cechy odróżniającej. Dla zagwarantowania prawidłowego funkcjonowania urządzeń w pełnym zakresie, koniecznie zaleca się zamknięcie pętli oprzewodowania magistrali wejścia / wyjścia (IO BUS).

W celu połączenia urządzeń i elementów systemu należy użyć oprzewodowania podanego w części rysynkowej. Od switch’a instalacji budynkowej do poszczególnych switch’ów rozmieszczonych na poszczególnych kondygnacjach należy prowadzić przewód kat. 5e F-UTP 4x2x0,5. Przewód YLY 2x2,5 mm2 należy prowadzić od zasilacza poprzez switch systemowy do każdego modułu sygnalizacji świetlnej. Od switch’ów do terminali, modułów elektronicznych oraz modułów sterowania oświetleniem należy prowadzić przewód kat. 5e UTP 4x2x0,5. Połączenia poszczególnych elementów takich jak przyciski przyzywowej, moduły świetlne, gniazda do modułów przyzywowych , przyciski kasujące należy połączyć przewodem kat. 5e UTP 4x2x0,5mm – 6 biegunowy kabel płaski.

Funkcjonalność systemu

Zaznaczenie obecności

Funkcja ta pokazuje stan obecności poszczególnych osób personelu pielęgniarskiego / lekarskiego, pozwalając jednocześnie na natychmiastową ich lokalizację i przekazanie im właściwych wiadomości. Informacja o zaznaczeniu obecności wskazywana jest za pomocą podświetlenia przycisku na terminalu komunikacyjnym / terminalu pokojowym, który został uaktywniony, jak i przez lampki sygnalizacyjne znajdujące się od strony korytarza. Zaznaczenie obecności dokonywane jest przez naciśnięcie przycisków „zaznaczenia obecności" umieszczonych na terminalach pielęgniarskich. Każda informacja o miejscu pobytu osób z personelu medycznego trafia także do stanowiska dyżurnego pielęgniarek (terminala oddziałowego), dając im tym samym możliwość natychmiastowej lokalizacji poszukiwanej w sytuacji krytycznej osoby.

Dla systemu przywołań świetlnych przewidziane zostały różne kolory zaznaczenia obecności, z których każdy wyróżnia inną rangę osoby:

- kolor zielony – obecność pielęgniarki w pomieszczeniu,
- kolor czerwony ciągły – przywołanie z pomieszczenia uruchomione przez osobę potrzebującą pomocy w celu przywołania pielęgniarki,
- kolor czerwony ciągły i biały – przywołanie z pomieszczenia WC uruchomione przez osobę potrzebującą pomocy w celu przywołania pielęgniarki,
- kolor czerwony migający i zielony ciągły- przywołanie z pokoju uruchomione przez personel
  w celu przywołania kolejnej osoby z personelu pielęgniarskiego,
- kolor niebieski ciągły – obecność lekarza w pomieszczeniu,
- kolor niebieski migający i zielony ciągły - przywołanie z pokoju uruchomione przez personel w celu przywołania lekarza.

Funkcja ta umożliwia personelowi odbieranie przywołań we wszystkich pomieszczeniach gdzie przewidziane są terminale komunikacyjne systemu przyzywowego. System sam wyszukuje właściwe osoby wg. kategorii personelu i im przesyła odpowiednie komunikaty o przywołaniach. Dodatkowo wciśnięcie przycisku zaznaczenia obecności w pokoju w którym wyzwolono alarm przywołania powoduje jego skasowanie, a przy zdalnym odbieraniu przywołań z wykorzystaniem komunikacji głosowej, jeżeli personel ma zamiar udać się na miejsce przywołania, wyłączenie obecności wyzwala funkcję przełączenia obecności.

Przywołanie z łóżka pacjenta

Sygnał ten zostaje wywołany przez chorego za pomocą przycisku „gruszkowego" montowanego w uchwycie pacjenta. Przywołanie to trafia wyłącznie do pielęgniarki i jest wskazywane przez zapalenie się czerwonej lampki sygnalizacyjnej. Przywołania kasowane będą po zaznaczeniu obecności na terminalu w miejscu przywołania.

Przywołanie awaryjne

Przywołanie to zostaje wywołane automatycznie, gdy wtyczka urządzenia przeznaczonego dla chorego zostanie specjalnie (akt wandalizmu), czy niechcący wyciągnięta z gniazda. Skasowanie tego rodzaju alarmu następuję poprzez naciśnięcie przycisku obecności na terminalu i wpięcie wtyczki przycisku pacjenta do modułu gniazdkowego.

Przywołanie z pokoju

Sygnał ten zostaje wywołany przez osoby dyżurne pełniące służbę na oddziałach w sytuacjach, kiedy potrzebują dodatkowej pomocy – pielęgniarki, salowej, czy lekarza. Przywołanie może być sprawdzone i skasowane przez pielęgniarkę na każdym terminalu pielęgniarskim, oddziałowym.

Przywołanie z łazienki i wc

Jest to szczególny rodzaj przywołań, wymagający natychmiastowej reakcji i tym samym posiadający specjalny priorytet w systemie. W przypadku takiego przywołania prawdopodobieństwo bezpośredniego zagrożenia zdrowia lub życia pacjenta jest bardzo duże, należy więc bezzwłocznie udać się na miejsce. Informacja o tym rodzaju przywołania trafia do pielęgniarki dyżurnej, sygnał świetlny w tym przypadku ma kolor biały (lampki w korytarzu).

Nagłe przywołanie z łóżka

Jest to przywołanie wyzwolone za pomocą znajdującego się przy łóżku przycisku pacjenta i przy zaznaczonej obecności personelu pielęgniarskiego w danym pomieszczeniu. Przywołanie trafia do drugiej pielęgniarki, może zostać przez nią potwierdzone i skasowane na terminalu komunikacyjnym, oddziałowym. System wskazuje to przywołanie jako czerwony migający sygnał świetlny na pokojowej lampce sygnalizacyjnej w korytarzu i sygnał dźwiękowy w szybkim rytmie.

Przywołanie lekarza

Jest to przywołanie wyzwolone przez pielęgniarkę z terminala komunikacyjnego w przypadku niezbędnej interwencji lekarza. Przywołanie to następuje przy zaznaczonej obecności pielęgniarki i trafia bezpośrednio do miejsca, gdzie aktualnie przebywa lekarz dyżurny. Informacja ta może zostać przez niego odebrana i potem skasowana na innym terminalu pielęgniarskim. System wskazuje to przywołanie za pomocą migającego niebieskiego sygnału świetlnego (lekarz) i sygnału dźwiękowego w szybkim rytmie.

Wyzwalanie alarmu krytycznego

Wyzwalany kiedy niezbędna jest interwencja ekipy reanimacyjnej. Wyzwalany jest poprzez naciśnięcie odpowiedniej kombinacji przycisków na terminalu: żółtego zaznaczenia obecności i niebieskiego wezwania lekarza. Przywołanie to ma najwyższy priorytet w systemie.

Priorytety przywołań

Opisane powyżej rodzaje przywołań są uporządkowane w schemacie priorytetowym, zgodnie z normą DIN VDE 0834. „Inteligencja" systemu zapewnia odpowiednią dystrybucję równocześnie pojawiających się przywołań:

- alarm krytyczny,
- przywołanie lekarza,
- przywołanie z łazienki lub WC,
- nagłe przywołanie z sali chorych,
- nagłe przywołanie z łóżka pacjenta,
- przywołanie pacjenta będącego pod opieką szczególną,
- przywołanie z sali chorych,
- przywołanie z łóżka pacjenta.

Integracja z systemem sygnalizacji pożaru

Zgodnie z rozporządzeniem ministra spraw wewnętrznych i administracji z dnia 7 czerwca 2010 roku w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów, dźwiękowy system ostrzegawczy projektuje się z wyłączeniem pomieszczeń intensywnej opieki medycznej, sal operacyjnych oraz sal z chorymi.

W celu usprawnienia procedury przygotowania personelu do podjęcia czynności związanych z ewakuacją pacjentów ze szpitala podczas pożaru, projekt przewiduje pokazywanie szczegółowych informacji o pożarze na wyświetlaczach urządzeń systemu przyzywowego gdzie personel zaznaczył swoją obecność (zalogował się) i/lub na wyświetlaczach telefonów medycznych przypisanych do danego oddziału.

Integracja z systemem telefonów medycznych

System łączności głosowej musi gwarantować wysoką dostępność, stąd preferowanym rozwiązaniem jest dedykowana sieć odbiorników/stacji/anten pracujących w oparciu o DECT.

Zastosowane rozwiązanie musi umożliwiać komunikację głosową zarówno w ramach systemu przyzwowego i komunikacji jak również z obsługą przemieszczającą się po obiekcie wyposażoną w telefony medyczne.

Rozwiązanie łączności głosowej w projekcie opierać się będzie również o niezależny od szpitalnego serwer połączeń głosowych. Owo rozwiązanie musi gwarantować połączenie po SIP bądź H323 z serwerem systemu przyzywowego oraz szpitalnym systemem centrali telefonicznej.

4.1.10 System bezprzewodowej łączności głosowej dla personelu - DECT

Założenia

Projekt przewiduje instalację systemu bezprzewodowej łączności głosowej dla personelu medycznego z funkcją obsługi alarmowych wiadomości tekstowych z systemy przyzywowego.

Rozwiązanie łączności bezprzewodowej powinno zapewniać komunikację głosową oraz odbiór wywołań alarmowych na ustalonej powierzchni szpitala oraz gwarantować elastyczną rozbudowę w przyszłości. Terminale dla personelu powinny być wykonane w technologii i z materiałów pozwalających na czyszczenie środkami antybakteryjnymi. System oprócz wysokiej jakości komunikacji głosowej, musi wspierać obsługę wiadomości tekstowych z zastosowanego systemu przyzywowego.

System łączności głosowej musi gwarantować wysoką dostępność, stąd preferowanym rozwiązaniem jest dedykowana sieć odbiorników/stacji/anten pracujących w oparciu o technologię DECT.

Zastosowane rozwiązanie musi umożliwiać komunikację głosową zarówno z użytkownikami systemu przyzywowego, jak również pozostałymi użytkownikami szpitala.

Rozwiązanie łączności głosowej w projekcie opierać się będzie również o niezależny od szpitalnego serwer połączeń głosowych. Owe rozwiązanie musi gwarantować połączenie po SIP, bądź H323 z serwerem systemu przyzywowego oraz szpitalnym systemem centrali telefonicznej.

Rozwiązanie systemu IP Dect musi zawierać wszelkie niezbędne do pracy serwery administracji, update, integracji z systemem przyzywowym oraz niezbędne licencje do zestawienia opisanej konfiguracji.

Stacje bazowe

System IP Dect składać się będzie z sieci stacji bazowych. Sieć stacji bazowych ma opierać się o jeden model urządzenia. Rozwiązanie IP Dect nie powinno pracować w oparciu o dedykowany kontroler. Stacje bazowe wpiętę będą do sieci LAN szpitala. Wymagane jest aby system stacji bazowych tworzył jedną sieć w ramach której, terminale personelu będą pracować w roamingu oraz wspierany będzie handover (przełączanie rozmowy w trakcie jej trwania podczas przejścia w zasięg innej anteny). Rozmieszczenie urządzeń do uzgodnienia podczas realizacji.

Rozwiązanie IP Dect ma umożliwiać samoczynną rekonfigurację gdy nastąpi uszkodzenie, odłączenie dowolnej stacji bazowej. Synchronizacja stacji bazowych musi odbywać się zarówno w powietrzu jak i poprzez sieć LAN.

Rozwiązanie IP Dect będzie współpracować z serwerem za pośrednictwem protokołu SIP oraz kodeku G.711.

Stacja bazowa IP Dect

- 8 kanałów rozmówych w kodeku G711,

- Zasilanie z PoE oraz opcjonalny zasilacz,
- Montaż naścienny,
- Minimum 1 kanał wiadomości tekstowych.

Terminale dla personelu medycznego

Personel pielęgniarski oraz lekarze będą wyposażeni w dedykowane terminale, pozwalające zarówno na realizację połączeń głosowych oraz odbiór alarmów z systemu przyzywowego. Wymagane jest aby terminal posiadał możliwość instalacji dodatkowych aplikacji pozwalających na rozszerzenie funkcjonalności systemu o integrację z innymi rozwiązaniami zastosowanymi w szpitalu.

Urządzenia powinny posiadać możliwość ustalenia restrykcji na obsługę usług, aplikacji, funkcji indywidualnie definiowanych dla wcześniej zdefiniowanych grup personelu.

Terminal powinien wspierać łączność „Walkie Talkie”/”Push To Talk”, umożliwiająca poprzez wciśnięcie jednego dedykowanego przycisku przesłanie komunikatu do ustalonej grupy użytkowników.

Każdy z terminali musi umożliwiać obsługę Bluetooth, NFC oraz posiadać fizyczny przycisk alarmowy, pozwalający na nagłe wezwanie pomocy przez użytkownika. Terminal musi umożliwiać usługę lokalizacji z wykorzystanie przynajmniej jednego z protokołów: RFID, BLE, DECT.

W projekcie przewidziano 20 terminali.

Terminal DECT

- Dotykowy wyświetlacz LCD minimum 3,5 cala
- Dodatkowy wyświetlacz w części czołowej urządzenia umożliwiający podglądanie zdarzeń bez wyjmowania telefony z kieszeni
- Klasa IP – IP54
- Obudowa antybakteryjna
- Kamera
- Wymienna bateria minimum 1600mA Li-Ion/Li-Po
- System operacyjny: Android umożliwiający instalowanie mobilnych aplikacji szpitalnych
- Klips
- Przycisk definiowany dla wezwania pomocy/alarmu
- Przycisk definiowany dla usługi PTT
- Fizyczne przyciski odbierania oraz zakończenia rozmowy
- NFC
- Bluetooth
- DECT
- WiFi 802.11 a/b/g/n
- Ładowarka biurkowa

Funkcjonalność

Rozwiązanie IP Dect musi posiadać, jeśli niezbędne, serwery pozwalające na:

- Zdalne zarządzanie terminalami pozwalające na rejestrację, definiowanie uprawnień, monitorowanie poprawności pracy, zdalny upgrade itp.

- Nadzór nad zainstalowanymi aplikacjami i możliwość ich zdalnego wgrywania oraz usuwania z terminala,
- Zdalny upgrade stacji bazowych,
- Integrację z systemem przyzywowym, konfigurację zdarzeń alarmowych odbieranych z systemu przyzywowego, z opcją przesyłania ich do systemu przyzywowego. System powinien pozwalać na dołączenie innych systemów powiadamiania, alarmowania w miarę rozwoju placówki,
- Odbieranie połączeń głosowych przychodzących z systemu przyzywowego,
- IP PBX pozwalający na obsługę połączeń głosowych na terminalach IP Dect oraz integrację poprzez SIP/H323 z systemem głosowym systemu przyzywowego obsługującego terminale pacjentów oraz główną centralą telefoniczną szpitala.
- Niezbędne licencję do uruchomienia opisanego scenariusza

Dopuszcza się aby system przyzywowy oraz system IP Dect pochodziły od innych producentów. Wymagane jest jednak aby producenci rozwiązań (nie dostawcy) pisemnie potwierdzili kompatybilność rozwiązań i poprawną współpracę.

4.1.11 System Wykrywania Gazów

Detekcja tlenku węgla

W pomieszczeniach strefa dostaw (P.627) oraz ciepła sień (0.020) projektuje się system wykrywania i pomiaru tlenku węgla oparty na centrali oraz detektorach CO. Centrala powinna umożliwiać podłączenie detektorów cyfrowych i detektorów analogowych. Centrala powinna umożliwić zaprogramowanie min. 4 progów alarmowych różnych dla każdego detektora, być wyposażona w min. 5 bezpotencjałowych wyjść stykowych (4 progi alarmowe oraz awaria) oraz min. 2 wyjścia analogowe 4-20 mA, które można dowolnie zaprogramować. Centrala powinna być wyposażona w układ samotestujący powiadamiający w przypadku awarii oraz układ monitorujący podłączone detektory. Panel czołowy centrali powinien być wyposażony w diody sygnalizujące zasilanie, min. 2 poziomy alarmu, awarię oraz przyciski nawigacji po menu. Centrala powinna zostać zamontowane w dedykowanej obudowie o stopniu ochrony IP66 wraz z zasilaczem 230/24. Do centrali w strefie dostaw należy podłączyć 4 detektory tlenku węgla pracujące na magistrali RS485, natomiast dla ciepłej sieci (0.020) przewidziano dwa detektory, które należy podłączyć do centrali znajdującej się w pom. ochrony (0.043). Detektory należy zamontować na wysokości 150-180cm nad poziomem podłoża, natynkowo, stosując okablowanie zgodne z instrukcją montażu. Detektory powinny być wyposażone w elektrochemiczne wymienne moduły sensoryczne. System powinien umożliwiać sygnalizację 4 progów alarmowych na poziomie 30ppm, 60ppm, 150ppm i 300ppm. 3 pierwsze progi mają być ustawione jako przeliczanie średniej ważonej, przy czym system powinien wyświetlać pomiar zarówno bieżący jak i pomiar średniej ważonej. System powinien spełniać wymagania normy PN-EN 50545-1, PN-EN 50271 oraz zapewniać poziom nienaruszalności bezpieczeństwa na poziomie SIL2. Detektory powinny być wykonane w klasie ochrony min. IP65. W pomieszczeniach oraz przed wjazdami do tych pomieszczeń należy zamontować podświetlane dźwiękowe tablice ostrzegawcze z piktogramem ewakuacji oraz napisem „STOP MOTOR”. Zasilanie tablic należy podać przez styk w centrali.

Dzięki zastosowaniu systemu z kilkustopniowym alarmowaniem możliwy jest następujący schemat alarmowania systemu detekcji:

- 30ppm – alarm I stopnia, sygnalizacji na wyświetlaczu centrali i w BMS,
- 60ppm – alarm II stopnia, włączenie wentylacji wywiewnej na II bieg,
- 150ppm – alarm III stopnia, sygnalizacja optyczna tablic.
- 300ppm – alarm IV stopnia, sygnalizacji akustyczna.

Sygnalizacje alarmów oraz awarii należy włączyć do szafy BMS, zgodnie z opracowaniem BMS.

Detekcja LPG

W pomieszczeniu strefa dostaw (P.627) projektuje się system wykrywania i pomiaru propan-butanu (LGP) oparty na centrali oraz detektorach LPG. Samochody wyposażone w instalację LPG będą miały zakaz wjazdu do strefy dostaw, jednak proponuje się wyposażenie tego obszaru w system detekcji. W tym celu należy wykorzystać projektowane detektory tlenku węgla i podłączyć do nich jako „slave" detektory LGP. Czujniki należy zamontować na wysokości ok 30cm nad poziomem podłoża, natynkowo, stosując okablowanie zgodne z instrukcją montażu. Detektory powinny być wyposażone w elektrochemiczne wymienne moduły sensoryczne, powinny pracować na magistrali RS485 i być wyposażone w wymienne sensory z zakresem pomiarowym 0-100% DGW (Dolnej Granicy Wybuchowości). System powinien umożliwiać sygnalizację 4 progów alarmowych na poziomie 10% DGW, 20% DGW, 30% DGW oraz 40% DGW. System powinien spełniać wymagania normy PN-EN 50545-1, PN-EN 50271 oraz zapewniać poziom nienaruszalności bezpieczeństwa na poziomie SIL2. Detektory powinny być wykonane w klasie ochrony min. IP65. Do alarmowania należy użyć tablic LED z wbudowanymi sygnalizatorami dźwiękowymi wspólnych dla systemu detekcji tlenku węgla.

Dzięki zastosowaniu systemu z kilkustopniowym alarmowaniem możliwy jest następujący schemat alarmowania systemu detekcji:

- 10% DGW – alarm I stopnia, sygnalizacji na wyświetlaczu centrali i w BMS,
- 20% DGW – alarm II stopnia, włączenie wentylacji wywiewnej na II bieg,
- 30% DGW – alarm III stopnia, sygnalizacja optyczna tablic.
- 40% DGW – alarm IV stopnia, sygnalizacji akustyczna.

Uwzględniając histerezę oraz granice błędów pomiarowych sugerowane jest stosowanie alarmowania co 10%.

Sygnalizacje alarmów oraz awarii należy włączyć do szafy BMS, zgodnie z opracowaniem BMS.

Zestawienia materiałów dla detekcji tlenku węgla i LPG

Strefa dostaw		
L.p.	**element**	**ilość**
1.	centrala	1
2.	detektor tlenku węgla	4
3.	detektor LPG	4
4.	podświetlana tablica LED z wbudowanym sygnalizatorem	3
5.	zasilacz 230V AC/24 V DC	1
6.	obudowa centrali	1
7.	okablowanie	kpl.
8.	pozostałe elementy montażowe	kpl.

Detekcja wodoru

W pomieszczeniach tech. IT (P.607), UPS i baterii (P.611), odb. ppoż (P.613) oraz UPS/sprężarkownia (P.246) projektuje się system wykrywania i pomiaru wodoru oparty na czujnikach H2 oraz centralach. Każda z central powinna umożliwiać podłączenie detektorów cyfrowych i detektorów analogowych. Powinna umożliwić zaprogramowanie min. 4 progów alarmowych dla każdego detektora, być wyposażona w min. 5 bezpotencjałowych wyjść stykowych (4 progi alarmowe oraz awaria) oraz min. 2 wyjścia analogowe 4-20 mA, które można dowolnie zaprogramować. Centrala powinna być wyposażona w układ samotestujący powiadamiający w przypadku awarii oraz układ monitorujący podłączone detektory. Panel czołowy centrali powinien być wyposażony w diody sygnalizujące zasilanie, min. 2 poziomy alarmu, awarię oraz przyciski nawigacji po menu. Centrale powinny zostać zamontowane w

dedykowanych obudowach wraz z zasilaczami 230/24. Do centrali w pom. P.607 należy podłączyć 4 detektory, do centrali w pom. P.611 należy podłączyć 4 detektory, natomiast do centrali w P.246 należy podłączyć 2 detektory. Detektory powinny pracować na magistrali RS485 i być wyposażone w wymienne sensory z zakresem pomiarowym 0-100% DGW (Dolnej Granicy Wybuchowości). Progi alarmowe powinny być ustawione na 4 poziomach 10%DGW, 20%DGW, 30% DGW i 40% DGW, aby stężenie gazu nie osiągało wartości mogących stanowić zagrożenie. W chronionych pomieszczeniach oraz przed wejściami do tych pomieszczeń należy zainstalować tablice ostrzegawcze z piktogramem „OPUŚCIĆ POMIESZCZENIE/LEAVE ROOM". Zasilanie tablic należy podać przez styki w centralach.

Dzięki zastosowaniu systemu z czterostopniowym alarmowaniem możliwy jest następujący schemat alarmowania systemu detekcji w trakcie ładowania akumulatorów:

- 0% DGW – brak alarmu, pracuje I bieg wentylacji (podstawowa wydajność),
- 10% DGW – alarm I stopnia, sygnalizacji na wyświetlaczu centrali, załączenie II biegu wentylacji (maksymalna wydajność),
- 20% DGW – alarm II stopnia, załączenie optycznego sygnału alarmowego,
- 30% DGW – alarm III stopnia, załączenie akustycznego sygnału alarmowego,
- 40% DGW – alarm IV stopnia, odłączenie prostowników

Detektory wodoru należy umieścić w najwyższych punktach pomieszczeń z uwzględnieniem tzw. „martwych stref" oraz elementów większych niż 30 cm (podpory, podciągi, itp.), które mogą dzielić górne części pomieszczenia na strefy. System powinien spełniać normy PN-EN 50271 oraz zapewniać poziom nienaruszalności bezpieczeństwa na poziomie SIL2. Detektory powinny być wykonane w klasie ochrony min. IP54.

W przypadku personelu obsługującego pomieszczenia chronione systemem detekcji i pomiaru wodoru, a także osób dokonujących przeglądów i konserwacji systemu, zasadnym jest, aby każda osoba wchodząca do chronionych pomieszczeń wyposażona była w personalny miernik gazów alarmujący w przypadku przekroczenia dopuszczalnego stężenia wodoru w powietrzu.

Sygnalizacje alarmów oraz awarii należy włączyć do szafy BMS, zgodnie z opracowaniem BMS.

Zestawienie materiałów dla detekcji wodoru

Pom. tech. IT P.607		
L.p.	**element**	**ilość**
1.	centrala	1
2.	detektor wodoru	4
3.	podświetlana tablica LED z wbudowanym sygnalizatorem	2
4.	zasilacz 230V AC/24 V DC	1
5.	obudowa centrali	1
6.	okablowanie	kpl.
7.	pozostałe elementy montażowe	kpl.

Pom. UPS i baterii P.611+pom. odb. ppoż. P.613		
L.p.	**element**	**ilość**
1.	centrala	1
2.	detektor wodoru	4
3.	podświetlana tablica LED z wbudowanym sygnalizatorem	3
4.	zasilacz 230V AC/24 V DC	1
5.	obudowa centrali	1
6.	okablowanie	kpl.

Pom. UPS i baterii P.611+pom. odb. ppoż. P.613		
L.p.	**element**	**ilość**
7.	pozostałe elementy montażowe	kpl.

Pom. UPS i baterii P.611		
L.p.	**element**	**ilość**
1.	centrala	1
2.	detektor wodoru	2
3.	podświetlana tablica LED z wbudowanym sygnalizatorem	1
4.	zasilacz 230V AC/24 V DC	1
5.	obudowa centrali	1
6.	okablowanie	kpl.
7.	pozostałe elementy montażowe	kpl.

Detekcja dwutlenku węgla

W pomieszczeniu rozprężalni CO2 (pom. 2.058) projektuje się system wykrywania i pomiaru dwutlenku węgla oparty na samodzielnym detektorze. Detektor powinien umożliwiać pracę bez centrali oraz umożliwiać wyposażenie w dodatkowe sensory gazów. Na panelu czołowym powinien mieć wyświetlacz zmieniający kolor przy wystąpieniu alarmu wraz z klawiaturą oraz diodami LED sygnalizującymi zasilanie, awarię oraz min. 2 progi alarmowe. Powinien umożliwiać dowolne zaprogramowanie progów alarmowych, emisję sygnału dźwiękowego i optycznego, posiadać wyjścia tranzystorowe 24CDC oraz bezpotencjałowe wyjścia styki 230VAC. Detektor należy wyposażyć w wymienny elektrochemiczny sensor dwutlenku węgla. Czujnik należy zamontować na wysokości ok 30cm nad poziomem podłoża, natynkowo, stosując okablowanie zgodne z instrukcją montażu. Detektor powinien być wykonany w klasie nienaruszalności bezpieczeństwa na poziomie SIL2 oraz w klasie ochrony min. IP65. Przed wejściem do pomieszczenia należy zamontować podświetlaną tablicę LED z napisem „Wyciek gazu" oraz z wbudowanym sygnalizatorem dźwiękowym. Zasilanie tablicy należy podać przez styk w detektorze.

Zastosowano następujący schemat alarmowania:

- 0,5% v/v – alarm I stopnia, sygnalizacja na wyświetlaczu detektora, w BMS oraz załączenie II biegu wentylacji (maksymalna wydajność),
- 1,5% v/v – alarm II stopnia, sygnalizacja optyczna i akustyczna na tablicy.

Zestawienie materiałów dla detekcji dwutlenku węgla

Pom. rozprężalni CO_2 (pom. 2.058)		
L.p.	**element**	**ilość**
1.	Samodzielny detektor dwutlenku węgla	1
2.	podświetlana tablica LED z wbudowanym sygnalizatorem	1
3.	okablowanie	kpl.
4.	pozostałe elementy montażowe	kpl.

Sygnalizacje alarmów oraz awarii należy włączyć do szafy BMS, zgodnie z opracowaniem BMS.

Wytyczne dla Użytkownika

System wykrywania gazu, zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. Nr 109 poz. 719), należy okresowo kontrolować i konserwować. Przeglądy powinny być przeprowadzane przez przeszkolony personel posiadający wymagane

prawem uprawnienia. Należy stosować czasookresy pomiędzy kontrolami systemu oraz kalibracją urządzeń zgodnie z DTR producenta urządzeń.

Minimalne parametry urządzeń

Centrala

- możliwość podłączenia do 96 detektorów cyfrowych (RS485)
- możliwość podłączenia do 32 detektorów analogowych (4-20mA)
- możliwość podłączenia detektorów do detekcji ponad 50 substancji wybuchowych, toksycznych, czynników chłodniczych lub tlenu
- pomiar z każdego detektora wyświetlany naprzemiennie na wyświetlaczu centrali z podziałem na pomiar bieżący i wartość średnią (ważne przy gazach toksycznych)
- 4 dowolnie ustawiane progi alarmowe
- 5 dowolnie ustawianych bezpotencjałowych wyjść stykowych o różnych opcjach zadziałania (4 alarmowe oraz awaria)
- 2 dowolnie ustawiane wyjścia analogowe (4-20mA)
- 4 diody LED sygnalizacji zasilania, awarii i 1 i 2 poziomu alarmu
- 6 przycisków do poruszania się po menu
- łatwa konfiguracja dzięki oprogramowaniu
- intuicyjne i proste menu w 6 dostępnych językach
- możliwość tymczasowego blokowania detektorów
- standardowa obudowa do montażu na szynę 35mm (wielkości 4 segmentów)
- gwarantowany poziom bezpieczeństwa SIL2
- zasilanie 24 VDC/AC -10% +20%
- zużycie prądu (bez opcji dodatkowych) 150mA, 4 W
- wejścia analogowe prądowe 4 – 20 mA, ochrona przed zwarciem i przeciążeniem, rezystor wejściowy 200Ω
- napięcie dla detektorów analogowych 24 VDC, max. 100mA / detektor
- wyjścia analogowe prądowe (2 szt.) 4 – 20 mA, ochrona przed zwarciem i przeciążeniem,
- rezystor wejściowy 500Ω
- przekaźnik alarmowy (4 szt.) 250 VAC, 5A, bezpotencjałowy, SPDT
- przekaźnik awarii (1 szt.) 250 VAC, 5A, bezpotencjałowy, SPDT
- wyświetlacz 2 liniowy, 16 znaków w linii, podświetlany
- diody LED (4 szt.) Zasilanie, awaria, alarm 1 i alarm 2
- nawigacja 6 przycisków na panelu czołowym
- transmisja danych RS 485
- gazy wg specyfikacji detektorów: wybuchowe, toksyczne, tlen

Detektor

- pomiar wartości widoczny na centrali
- komunikacja cyfrowa
- wymienne sensory w technologii X-Change
- duża odporność na warunki zewnętrzne IP65
- spełnia PN-EN-50271, PN-EN-50545
- poziom bezpieczenstwa SIL2
- zasilanie 16-28 VDC/AC (wbudowana ochrona przed odwrotną polaryzacją)

- zużycie prądu sensora Wg tabeli (bez opcji dodatkowych)
- zużycie prądu płyty detektora (SB) 10mA (0,24VA) (bez opcji dodatkowych)
- wyjscie dla detektora slave (RB) 5VDC, 250mA max.
- komunikacja RS485
- wilgotność dla płyty detekotra (SB) 15-90 % RH bez kondensacji
- temperatura dla płyty detektora (SB) -35oC - +50oC (-31oF - +120oF)

Ciśnienie:

- Sensory PE 800-1200hPa (atmosferyczne 1013hPa ±20%)
- Sensory EC 800-1200hPa (atmosferyczne 1013hPa ±20%)
- Sensory IR 700-1300hPa (atmosferyczne 1013hPa ±30%) wpływ +1,6% mierzonej wartości na każdy kPa
- Sensory SC 800-1100hPa (atmosferyczne 1013hPa ±20%)

Oznaczenia sensorów:

- IR Sensor podczerwony
- PE Sensor katalityczny
- EC Sensor elektrochemiczny
- SC Sensor półprzewodnikowy
- Obudowa z tworzywa poliwęglan
- Palność UL 94 V2

Podświetlana tablica LED

Tablica musi zapewniać widoczność w różnych warunkach oświetlenia. Montaż do ściany, sufity lub jako wiszący. Zasilanie poprzez styk w centrali/detektorze. Treść wyświetlanego napisu uzgodnić z Użytkownikiem. Wbudowany sygnalizator akustyczny.

4.1.12 Instalacja RTV

W obiekcie projektuje się sieć TV naziemnej. Dostęp do telewizji przewiduje się w pomieszczeniach łóżkowych, świetlicach oraz innych lokalizacjach wg projektu technologii. Lokalizacja gniazd abonenckich zgodnie z częścią rysunkową.

Część antenowa

Antenę telewizji naziemnej projektuje się na dachu nadbudówki budynku. Antena powinna być zamontowana za pomocą dedykowanych uchwytów do konstrukcji dachu. Elementy anteny muszą być zabezpieczone antykorozyjnie. Antena powinna umożliwiać odbiór programów cyfrowej telewizji naziemnej DVB-T.

Okablowanie od anteny do węzła magistralnego na ostatniej kondygnacji w pomieszczeniu teletechnicznym 5.604 należy wykonać kablami koncentrycznymi typu KH. Wszystkie kable wchodzące do budynku należy zabezpieczyć przeciwprzepięciowo dedykowanym zabezpieczeniem do instalacji multiswitchowych.

Stacja czołowa

Stacja czołowa umożliwi modulację sygnału DVB i BVB-S/S2 do transmisji QAM. Stacja umożliwi obsługę do 24 programów. Stacja składa się ze stacji bazowej (cabinet) z zasilaczem dla 16 frontend i 6 back-end, modułów wejściowych (frontend) DVB-T/T2 MPG-4 i modułu wyjściowego (backend) – modulator pełnopasmowy 47-862 MHz. Sygnały z modułów wejściowych podawane są do części wspólnej. W przypadku projektowanej stacji dowolny sygnał z modułów wejściowych może być podany na dowolny modulator wyjściowy. Dzięki temu Użytkownik może w optymalny sposób tworzyć swoje własne „paczki programów” dla poszczególnych modulatorów. Zastosowana stacja czołowa spełnia warunek możliwości

zdalnego zarządzania poprzez połączenie internetowe. Możliwość przetwarzania/multipleksowania sygnałów wejściowych na dowolny sygnał wyjściowy zapewnia stacji czołowej elastyczność, efektywność oraz ekonomiczność. Możliwe jest również wyjście ze stacji jednocześnie więcej niż jednym rodzajem modulacji, np. COFDM i PAL, QAM i COFDM, QAM i PAL, itp. Stacja przeznaczona jest dla sieci od 10 do ponad 10000 odbiorców.

W przypadku zwiększenia liczby programów stację będzie można rozbudować za pomocą dedykowanych paneli wyjściowych. Stację czołową należy zlokalizować w pom. 5.604.

Poziom sygnału wymagany do prawidłowego odbioru naziemnej cyfrowej telewizji wynosi od 48 do 74 dBµV przy dostępnej modulacji 64-QAM, FEC ¾. W poniższej tabeli przedstawiono poziom sygnałów instalacji RTV.

Sygnał cyfrowy z anteny TV naziemnej		**80,00 dB**
	Tłumienie kabla pionowego zewnętrznego 4m	0.52 dB
	Tłumienie odgromnika liniowego	3,00 dB
	Tłumienie kabla pionowego wewnątrz 35m	5.2 dB
Wejście stacji czołowej	Poziom sygnał wejściowego stacji czołowej	**71,28 dB**
Wyjście stacji czołowej	Poziom sygnału wyjściowego stacji czołowej	**90 dB**

Okablowanie

Pomiędzy anteną a stacją czołową należy poprowadzić 12 kabli koncentrycznych o grubości żyły głównej 1,1-1,63 i skuteczności ekranowania nie mniejszej niż 85 dB. Przewody należy prowadzić na projektowanych teletechnicznych trasach kablowych.

Sygnał w węźle magistralnym po wzmocnieniu zostanie poprowadzony do poszczególnych węzłów dystrybucyjnych szachtowych/piętrowych. Magistrale zostały poprowadzone kablem magistralnym typu TC-11 z węzłów magistralnych do węzłów dystrybucyjnych zlokalizowanych w poszczególnych pomieszczeniach teletechnicznych na danym piętrze (zgodnie ze schematem blokowym). Sygnał w punktach dystrybucyjnych na poszczególnych kondygnacjach został rozdzielony na poszczególne gniazda za pomocą multiswitchy.

System opcjonalnie powinien umożliwiać podłączenie telewizji kablowej wybranego przez Użytkownika operatora. W tym celu należy przewidzić światłowód jednomodowy, min. 4J z pomieszczenia stacji czołowej na P05 do pom. przyłącza na B01. Takie podłączenie nie może skutkować modyfikacjami instalacji, należy wykorzystać projektowane urządzenia.

Zarządzanie

System należy wyposażyć w centrum sterowania telewizorami (serwer). Serwer należy zamontować w szafie RACK w pomieszczeniu wraz ze stacją czołową (PPD.5.2). Rozwiązanie musi być kompatybilne z instalowanymi na obiekcie telewizorami, tak aby zapewnić możliwości:

- zdalnego konfigurowania telewizorów,
- tworzenia spersonalizowanych szablonów z informacjami oraz automatyczne ich przesyłanie do wybranych TV,
- tworzenia kanału powitalnych,
- grupowego zarządzania poszczególnymi odbiornikami, ich ustawieniami i aktualizacjami,
- wyświetlania wiadomości, reklam, jednoprzyciskowego zamiawiania usług na ekranie,
- trybu klonowania: replikowanie funkcji komunikacji i dostarczania treści na wybranych lub wszystkich telewizorach.

4.1.13 Instalacja audio-wizualna sal konferencyjnych

W obiekcie projektuje się instalację audio-wizualną AV umożliwiającą realizację wideokonferencji. Instalację przewiduje się w centrum dydaktyczno-konferencyjnym, w którym sala konferencyjna będzie miała możliwość podziału na dwie mniejsze z zachowaniem funkcjonalności odrębnych sal, a także w sali konferencyjnej działu administracji.

W skład opracowania wchodzą następujące systemy:

- System prezentacji obrazów,
- System nagłośnienia,
- System zintegrowanego sterowania AV i transmisji sygnałowej,
- System zarządzania urządzeniami AV,
- System zarządzania wyposażeniem multimedialnym,
- System wideonferencyjny.

Założenia programowe i funkcjonalne sal konferencyjnych

Główne założenia programowe i funkcjonalne:

- wyświetlanie prezentacji multimedialnych,
- nagłośnienie prezentacji multimedialnych,
- sterowanie wyposażeniem multimedialnym,
- sterowanie oświetleniem,
- komunikacja BACnet,
- System Zarządzania powinien umożliwiać kompleksowe zarządzanie wszystkimi systemami składowymi,
- prowadzenie konferencji, prezentacji multimedialnych, szkoleń itp.,
- łatwość obsługi i automatyka dostosowania systemów zgodnie z wymogami Użytkownika,
- oferowanie rozwiązań praktycznie zweryfikowanych w realizacjach podobnych obiektów o wysokim standardzie wyposażenia,
- możliwość nadzoru i zarządzania wyposażeniem multimedialnym,
- wymagana jest spójność i wysoka niezawodność systemu dlatego system dystrybucji sygnałów AV wraz z systemem sterowania ma być jednego producenta.
- Komunikacja BACnet z obu sal – przekazywanie statusów do systemu BMS o roletach i świetle.

Wyposażenie – sala konferencyjna 2.505

Sala z możliwością podziału na 2 sale oraz wydzieleniem korytarza.

W pomieszczeniu zostaną zainstalowane wysokiej klasy 3 projektory multimedialne LCD Full HD. Na projektorach po podłączeniu się urządzeniami źródłowymi do zainstalowanych przyłączy AV będzie można wyświetlać obrazy w dowolnej konfiguracji. Na wszystkich ekranach ten sam obraz lub na każdym ekranie inny (z różnych przyłączy AV). Pod biurkiem należy przewidzieć dodatkową puszkę podłogową jako magazyn dla nadajnika sygnałowego.

Ekrany projekcyjne zostaną wbudowane w sufit podwieszany dzięki czemu obudowa nie będzie wystawała i będzie zlicowana.

Na sali gdzie zostaną zainstalowane 2 zestawy projekcyjne zostały przewidziane 2 przyłącza stołowe na siłowniku wyposażone w złącze VGA audio oraz HDMI, a na sali w tylnej części zaprojektowano przyłącze ścienne wyposażone m.in. w złącze vga/audio oraz HDMI.

Ponadto na każdej z sal będzie można wyświetlić sygnał TV z dostępnego w szafie rack tunera.

Do nagłośnienia sal przewidziano 20 kolumn sufitowych do zabudowy. Do dyspozycji prelegentów będą 2 mikrofony przewodowe z podstawą oraz 2 mikrofony bezprzewodowe do ręki. Za poprawne dotarcie sygnału z mikrofonów bezprzewodowych do jednostki centralnej odpowiadać będą zewnętrzne anteny mikrofonowe zainstalowane na sali.

Oprócz parametrów technicznych istotne są parametry funkcjonalne, wygląd urządzeń i ich dopasowanie do aranżacji wnętrza.

Sala zostanie wyposażona w system sterowania urządzeniami AV, zaciemnieniem, roletami oraz oświetleniem. Zarządzanie odbywać się będzie za pomocą ściennego panelu dotykowego o wielkości 5". Przy drzwiach wejściowych zostaną zainstalowane klawiatury sterujące oświetleniem. Należy przewidzieć możliwość sterowania oświetlenia dla całej sali jak i dla wydzielonych dwóch sal osobno.

Dodatkowo sala została wyposażona w system wideokonferencyjny umożliwiający komunikację z oddalonymi lokalizacjami. Jednocześnie może się połączyć do 6 lokalizacji. Jedna kamera będzie zlokalizowana pomiędzy ekranami natomiast druga na ścianie (obie na wysokości ok 250 cm).

Wyposażenie – sala konferencyjna 5.011

W pomieszczeniu zostanie zainstalowany wysokiej klasy projektor multimedialne LCD Full HD. Na projektorze po podłączeniu się urządzeniami źródłowymi do zainstalowanych przyłączy AV będzie można wyświetlać obraz. Projektuje się 2 przyłącza stołowe na siłowniku każde wyposażone w m.in. vga/audio, HDMI. Pod stołem należy przewidzieć dodatkową puszkę podłogową jako magazyn dla nadajnika sygnałowego.

Ekran projekcyjny zostanie wbudowany w sufit podwieszany dzięki czemu obudowa nie będzie wystawała i będzie zlicowana.

Ponadto na sali będzie można wyświetlić sygnał TV z dostępnego w szafie rack tunera.

Do nagłośnienia sali przewidziano 6 kolumn sufitowych do zabudowy. Do dyspozycji prelegentów będzie mikrofon bezprzewodowy do ręki. Za poprawne dotarcie sygnału z mikrofonów bezprzewodowych do jednostki centralnej odpowiadać będą zewnętrzne anteny mikrofonowe zainstalowane na sali.

Oprócz parametrów technicznych istotne są parametry funkcjonalne, wygląd urządzeń i ich dopasowanie do aranżacji wnętrza.

Sala zostanie wyposażona w system sterowania urządzeniami AV, zaciemnieniem oraz oświetleniem. Zarządzanie odbywać się będzie za pomocą ściennego panelu dotykowego o wielkości 5". Przy drzwiach wejściowych zostaną zainstalowane klawiatury sterujące oświetleniem.

Dodatkowo sala została wyposażona w system wideokonferencyjny umożliwiający komunikację z oddalonymi lokalizacjami. Jednocześnie może się połączyć do 6 lokalizacji. Kamera będzie zlokalizowana będzie na przedniej ścianie.

Elementy systemu

Elementem sterującym będą panele dotykowe oraz klawiatury sterujące. W pamięci jednostki centralnej w trakcie instalowania i programowania systemu zapisane będą programy wykonawcze. Programy te, definiujące funkcje poszczególnych okien i przycisków panelu dotykowego sterują funkcjami poszczególnych urządzeń oraz wykonują MAKROPROGRAMY - sekwencje instrukcji uruchamianych po naciśnięciu jednego klawisza – np. LAPTOP spowoduje rozwinięcie się ekranu i załączenie wideoprojektora oraz uruchomienie źródła, zatrzymanie innych źródeł, ustawienie wymaganego poziomu głośności prezentacji multimedialnych oraz np. odpowiednie oświetlenie sali (Makroprogramy prezentacji multimedialnych będą dedykowane do pomieszczeń, w których jest zaprojektowany system sterowania).

Przyłącze aktywne w danym momencie, będzie posiadać swoje odzwierciedlenie na panelach sterujących odpowiednią sygnalizacją.

Liczba przepracowanych godzin przez projektor będzie wyświetlana na panelu. Harmonogram czasowy włączania i wyłączania systemu np. system aktywny od godz 6:00, wyłączenie systemu godz 22:00.

Minimalne parametry urządzeń

Projektor typ1

- Technologia - 3LCD
- Natężenie światła - min. 5500 lumenów
- Rozdzielczość - WUXGA (1920 x 1200)
- Współczynnik proporcji - 16:10
- Stosunek kontrastu - min. 15000:1
- Żywotność lampy min. 5000 h w trybie normalnym
- obiektyw z optyką w zakresie 1,3-2,3:1
- Lens-Shift - pionowo +/-50%; poziomy +/- 10% ;
- Wejścia: VGA, HDBaseT, HDMI x 2, Audio mini jack, RS-232, LAN, USB 2.0, - Wyjścia: VGA, Audio mini jack
- oryginalna wysłona przykręcana do projektora ukrywająca podłączone okablowanie

Uchwyt do projektora typ1

- 4 punkty mocowania
- Blacha o grubości 3 mm malowana proszkowo
- Teleskopowa konstrukcja uchwytu o profilu okrągłym
- Możliwość regulacji min. 48-60 cm, kolor biały,
- Korekta lewo/prawo 18°/18°
- Regulacja kąta nachylenia 90°/90°,
- Prowadzenie okablowania wewnątrz uchwytu
- malowany proszkowo na kolor biały

Przyłącze stołowe A

- Przyłącze otwierane pneumatycznie
- 1 x Gniazdo zasilania ~230V
- 1 x Gniazdo komputerowe VGA
- 2 x Gniazdo Ethernetowe RJ-45
- 1 x Gniazdo HDMI
- 1 x Gniazdo audio mini Jack

Przyłącze stołowe B

- Przyłącze otwierane pneumatycznie
- 1 x Gniazdo zasilania ~230V
- 1 x Gniazdo komputerowe VGA
- 2 x Gniazdo Ethernetowe RJ-45
- 1 x Gniazdo HDMI
- 1 x Gniazdo audio mini Jack

Kabel VGA+audio 2m

- Złącza VGA/Audio-VGA/Audio, męsko-męskie
- Przewód VGA z zintegrowanym przewodem audio 3,5 mm
- Obsługa rozdzielczości do 1920*1200
- Wysoko elastyczny przewód
- Potrójnie ekranowany przewód
- Długość przewodu - 2m

Kabel HDMI 2m

- Złącza HDMI-HDMI, męsko-męskie
- Obsługa rozdzielczości do 4K * 2K@60Hz
- Wysoko elastyczny przewód
- Obsługa ARC, 3D, HDCP, CEC
- Zawartość miedzi w przewodzie min. 99,99%
- Potrójnie ekranowany przewód
- Pozłacane złącza
- Długość przewodu - 2m

Nadajnik sygnałowy

Urządzenie transmitujące sygnał AV po skrętce na odległość 100m, posiadające wbudowany automatyczny switcher, złącza na wyposażeniu:

- 1 x wejście RJ-45 LAN
- 1 x wyjście RJ-45 obsługujące transmisję sygnału po skrętce
- 1 x wyjście HDMI
- 1 x wejście HDMI
- 1 x wejście VGA/DB15HD
- 1 x wejście mini jack Audio
- Obsługa HDCP, EDID, CEC, IEEE 802.3at, Ethernet, HDBaseT
- Kontrolki LED sygnalizujące sygnały źródłowe oraz aktywny odbiornik

Tuner TV

- Obsługiwana rozdzielczość min. FullHD
- Skalowanie sygnału PAL do rozdzielczości 1080p
- Dźwięk Dolby Digital Plus
- Obsługa standardów MPEG-2, MPEG-4, MPEG-4 AVC/H.264
- Kompatybilny z systemami DVB-S, DVB-S2, DVB-C, DVB-T i DVB-T2
- Gniazdo CI
- Jednoczesne oglądanie jednego i nagrywanie drugiego kanału
- Możliwość zapisu na dysk zewnętrzny USB
- Wejście kabla antenowego, Wyjście sygnału cyfrowej TV naziemnej do innego odbiornika, Wyjście HDMI, Wejście USB, Wejście LAN, Wejście RS-232, Wyjście SPDIF, Wyjście Audio
- Pilot w zestawie

Przyłącze HDMI, VGA+MIC, MICVK wypełnienie floorboxa

Zakończenie okablowanie we floorboxie złączami HDMI (moduł 45x45 w poziomie), VGA/audio (moduł 45x45 w poziomie), XLR, złącze mikrofonowe zgodne z mikrofonami producenta wideokonferencji.

Kolumna sufitowa

Dwudrożne głośniki sufitowe, wbudowany transformator napięcia pozwala na pracę w trybie 100V lub 8Ω, Polypropylenowe woofery zapewniają odporność produktu na ciepło i wilgoć, zdejmowalna maskownica przystosowana do malowania, sprężynowe przyłącza wejściowe, pasmo przenoszenia w zakresie min 60Hz-20kHz, moc min 30W przy 100V, waga max 2,5 kg.

Wzmacniacz mocy

- moc 2x150W przy 100V
- chłodzenie bezwentylatorowe
- pokrętła regulujące głośność na przednim panelu
- pasmo przenoszenia min 20Hz - 30kHz
- zabezpieczenie termiczne

Mikrofon bezprzewodowy

Nadajnik:

- zakres częstotliwości transmisyjnych: UHF zgodny z odbiornikiem
- zakres zmian częstotliwości transmisyjnej: > 40 MHz
- skok przestrajania: 25 kHz
- moc wyjściowa w.cz.: ≥ 30 mW
- rodzaj przetwornika mikrofonowego: dynamiczny kardioidalny
- maksymalny poziom wysterowania 154 dB SPL
- pasmo przenoszenia m.cz.: 80÷18 000 Hz
- zakres zmian czułości wejściowej nadajnika: 40 dB
- tryb przełączania czułości wejściowej: skokowo, skok ≤ 6 dB
- zniekształcenia nieliniowe: < 1 %
- stosunek sygnał/szum: 110 dB(A)
- wyświetlacz ze wskazaniem częstotliwości transmisyjnej
- poziomu wysterowania audio
- stanu naładowania ogniw zasilających
- port podczerwieni do synchronizacji z odbiornikiem: częstotliwości transmisyjnej
- zasilanie: 2 ogniwa AA
- czas pracy z 1 kompletu ogniw≥ 8 h
- rodzaj obudowy: metalowa

Odbiornik:

- system odbioru: dwu-antenowy różnicowy „true diversity”
- zakres częstotliwości transmisyjnych: UHF
- zakres zmian częstotliwości transmisyjnej: > 40 MHz
- skok przestrajania: 25 kHz
- pasmo przenoszenia m.cz.: 25 ÷ 18 000 Hz.
- zniekształcenia nieliniowe: ≤ 1 %

- stosunek sygnał/szum: ≥ 110 dB(A)
- typ złącza wyjściowego sygnału audio, standard sygnału : XLR, sygnał symetryczny
- poziom sygnału wyjściowego przy dewiacji nominalnej: ≥ 12 dBu
- wyświetlacz ze wskazaniem: częstotliwości transmisyjnej
- poziomu sygnału antenowego
- poziomu wysterowania audio
- stanu naładowania ogniw nadajnika
- skanowanie pasma z wyszukiwaniem niezakłóconych częstotliwości transmisyjnych
- port podczerwieni do synchronizacji z nadajnikiem: częstotliwości transmisyjnej
- typ złączy antenowych: BNC
- rodzaj obudowy: metalowa, montowalna w panel 1U, 19”

Statyw biurkowy

- podstawa żeliwna lakierowana strukturą krystaliczną na czarno, -wysięgnik teleskopowy 30/50cm
- rury stalowe
- lakier proszkowy czarny półmat
- waga min 2,6kg

Jednostka centralna

Przełącznik matrycowy 8x4:

- wbudowany procesor umożliwiający zintegrowanie systemu oraz programowalne sterowanie pomieszczeniem
- wbudowany skaler 4K (4096 x 2160@ 60 Hz)
- transmisja sygnału po skrętce na odległość 100 m, w tym również dla sygnału 4K
- wbudowany min. 6 kanałowy przedwzmacniacz mikrofonowy z zasilaniem Phantom 48V,
- wbudowany procesor dźwięku DSP,
- wbudowany wzmacniacz 70V/100V,
- zarządzanie informacjami EDID między urządzeniami wyświetlającymi i źródłami wejściowymi,
- obsługa aplikacji sterujących dla systemów iOS, Android oraz poprzez przeglądarkę internetową,
- obsługa HDBaseT, HDCP 2.2, CEC, 3D, 4K, Ethernet, PoE+ dla wejść/wyjść HDBaseT, DTS-HD Master Audio
- możliwość instalacji w szafie rack 19", wysokość maks. 3U
- pamięć flash min. 4 GB
- 2 x złącze DB9 obsługujące dwukierunkową transmisje RS-232
- 1 x złącze 8 pinowe obsługujące 4 nadajniki podczerwieni
- 4 x złącze obsługujące magistralę systemową
- 1 x złącze LAN (RJ45)
- 1 x złącze USB do programowania jednostki
- 1 x złącze 8 pinowe obsługujące 4 izolowane przekaźniki
- Wejścia sygnałowe: 2x RJ45 z obsługą HDBaseT, 6 x HDMI, 5 x Audio, 6 x Mikrofonowe

- Wyjścia sygnałowe: 2 x HDMI, 2 x RJ45 z obsługą HDBaseT, 3 x Audio, wyjście głośnikowe
- komunikacja BACnet

Panel sterujący 5”

5" ekran dotykowy TFT zasilany POE zamontowany na ścianie do puszki montażowej podtynkowej wyposażony dodatkowo w pięć przycisków, wbudowany mikrofon, wbudowany głośnik, obsługa formatu H.264, jasność min 400 cd, 5 punktowy multitouch, intercom, wyświetlanie strumieniowanego obrazu wideo. Montowany na puszcze montażowej podtynkowej.

Zasilacz PoE

- Zgodne ze standardem 802.3af oraz 802.3at
- Port wejścia RJ-45 1000 Mb/s
- Port wyjścia danych oraz zasilacza 1000 Mb/s

Klawiatura sterująca

- Możliwe konfiguracje przycisków: 4, 6.
- 1x złącze magistrali systemowej
- Zintegrowany fotosensor
- 2x wejście cyfrowe
- Zasilanie poprzez magistralę systemową
- W zestawie z klawiaturą: 2x paski przycisków średnich (po 3 przyciski), 2x paski przycisków dużych (po 2 przyciski)
- Kolor biały lub czarny

Moduł przekaźnikowy

- ilość przekaźników (kanałów): 8.
- Maksymalne obciążenie dla opraw świetlówkowych na kanał: 5A.
- Maksymalne obciążenie dla opraw żarowych na kanał: 10A.
- Maksymalne obciążenie rezystancyjne: 16A.
- 2 porty override.
- Port magistrali komunikacyjnej kompatybilny z innymi urządzenia systemu sterowania.
- Przystosowany do pracy 230V/50Hz.
- Zasilanie: 24V DC poprzez port magistralowy.
- Konfiguracja poprzez panel frontowy lub oprogramowanie.
- Wskaźniki LED informujące o: komunikacji, zasilaniu, trybie override, statusie każdego kanału.
- Wyświetlacz numeryczny wskazujący numer identyfikacji w sieci.
- Przycisk resetujący wewnętrzny procesor.
- Możliwości montażowe: montaż na szynie DIN, szerokość 9 modułów DIN.

Zasilacz systemowy 50W

Zasilacz systemowy na szynę DIN o mocy min 50 W 24V, do zasilenia urządzeń podłączonych do magistrali systemowej wyposażony w 3 porty magistrali systemowej.

Moduł sterowania oświetleniem

Moduł sterowania oświetleniem montowany na szynę DIN dla 2 niezależnych pętli DALI. Obsługa na jednej linii do 64 stateczników. Zintegrowany zasilacz magistrali Dali. Możliwość wysterowania poprzez jednostkę centralną systemu sterowania. Wyświetlacz numeryczny wskazujący numer identyfikacji w sieci. Komunikacja z procesorem sterującym poprzez magistralę sterującą lub/oraz sieć ethernet. Wyposażony w 2 porty magistrali systemowej, montaż na szynie DIN, szerokość 9 modułów DIN, wejście Override, port Ethernet.

Router

- Procesor: min 2 rdzenie, min 1.4 GHz
- 10 gigabitowych portów Ethernet
- 1 port SFP;
- 1 port USB 3.0;
- dotykowy ekran;
- wyjście PoE;
- możliwość montażu w szafie RACK;
- monitorowanie napięcia;

Zestaw wideokonferencyjny

Oprogramowanie umożliwiające połączenie 6 punktów, oprogramowanie dla urządzeń mobilnych.

Mostek: Obsługa 6 lokalizacji, obsługa rozdzielczości 1080p, obsługiwana liczba klatek na sekundę 1080p 60 kl./s, wejścia HDMI x1, DVI-Dx2, wyjścia HDMI x 2, DVI-I x 1, port RS 232, zdalne sterowanie kamerą, podwójne strumieniowanie, protokoły komunikacyjne H.263, H.263+, H.263++, H.264, MPEG-4, Eliminacja echa w dźwięku stereo, automatyczna regulacja wzmocnienia, redukcja szumu.

Porty sieci 10BASE-T/100BASE-TX/1000BASE-T x 2, interfejs ISDN x 1.

Mikrofony: 2 mikrofony przewodowe o charakterystyce dookólnej działające 360 stopni, pasmo przenoszenia o szerokości min 14 kHZ.

Kamera: Przetwornik obrazu CMOS, powiększenie optyczne min 12x, kąt widzenia w poziomie min 70 stopni, szybkość obrotu min 280 stopni na sekundę, pochylenie min 125 stopni na sekundę, przetwornik obrazu min 2 megapiksele.

Obsługa przez system główny maksymalnie 8 połączeń z aplikacją.

Nadajnik sygnałowy ścienny

Urządzenie transmitujące sygnał AV 4K (4096x2160) po skrętce na odległość 100m, przeznaczone do zabudowy ściennej, złącza na wyposażeniu:

- 1 x wejście HDMI
- 1 x wejście RS-232 dwukierunkowe
- 1 x wyjście IR
- 1 x wyjście RJ-45 obsługujące transmisję sygnału po skrętce
- Obsługa HDCP 2.2, EDID, CEC, IEEE 802.3at, 3D, 4K, HDBaseT
- Kontrolki LED sygnalizujące sygnał źródłowy oraz aktywny odbiornik

Odbiornik transmisji ścienny

Urządzenie odbierające sygnał AV 4K (4096x2160) po skrętce na odległość 100m, przeznaczone do zabudowy ściennej, złącza na wyposażeniu:

- 1 x wejście RJ-45 obsługujące transmisję sygnału po skrętce
- 1 x wyjście HDMI
- 1 x wyjście RS-232 dwukierunkowo
- 1 x wyjście IR
- 1 x wyjście Ethernet
- Obsługa HDCP 2.2, EDID, CEC, IEEE 802.3at, Ethernet, HDBaseT, 3D, 4K
- Kontrolki LED sygnalizujące sygnał źródłowy oraz aktywne wyjście

Szafa RACK 22U

Cechy:

- Szafa stojąca 19" przeznaczona do zastosowań wewnątrz pomieszczeń.
- Wysokość 22U.
- Głębokość 600mm.
- Drzwi przednie z szybą z hartowanego szkła oraz zamkiem jednopunktowym.
- Drzwi tylne metalowe z zamkiem.
- Możliwość szybkiego przełożenia drzwi z lewych na prawe.
- Zdejmowane i zamykane na klucz panele boczne.
- Wsporniki do montażu wyposażenia 19" z przodu i z tyłu.
- Przepusty kablowe na górze i dole szafy.
- Profile montażowe ze stali ocynkowanej.
- Maksymalne obciążenie szafy : statyczne-800 kg , dynamiczne-400 kg.
- Możliwość zamontowania wentylatora.

Wykonanie:

- Precyzyjne i solidne wykonanie z wysokiej jakości stali SPCC, rama spawana.
- Grubość blach: 2,0mm profile montażowe, 1,2mm. pozostałe elementy.
- Wymiary: 600x600x1175mm. (szerokość x głębokość x wysokość).
- Kolor: czarny RAL 9004

W zestawie:

- 4 szt. nóżek i 4 szt. kółek.
- 4 komplety kluczy do drzwi.
- Zaślepki do przepustów kablowych.

Szafa RACK 42U

Cechy:

- Szafa serwerowa rack stojąca 19" przeznaczona do zastosowań wewnątrz pomieszczeń.
- Wysokość 42U.
- Głębokość 800mm.
- Drzwi przednie z szybą z hartowanego szkła oraz zamkiem jednopunktowym.
- Drzwi tylne metalowe z zamkiem.
- Możliwość szybkiego przełożenia drzwi z lewych na prawe.
- Zdejmowane i zamykane na klucz panele boczne.
- Wsporniki do montażu wyposażenia 19" z przodu i z tyłu.
- Przepusty kablowe na górze i dole szafy.
- Profile montażowe ze stali ocynkowanej.

- Maksymalne obciążenie szafy: statyczne-800 kg , dynamiczne-400 kg.
- Możliwość zamontowania wentylatora.

Wykonanie:

- Precyzyjne i solidne wykonanie z wysokiej jakości stali SPCC, rama spawana.
- Grubość blach: 2,0mm profile montażowe, 1.2mm. pozostałe elementy.
- Wymiary: 800x800x2020mm. (szerokość x głębokość x wysokość).
- Kolor: czarny RAL 9004

W zestawie:

- 4 szt. nóżek i 4 szt. kółek.
- 4 komplety kluczy do drzwi.
- Zaślepki do przepustów kablowych

Półka 45cm

- Półka 19" wzmocniona o wysokości 1U z regulowanymi uchwytami montażowymi charakteryzująca się wysoką wytrzymałością statyczną. Obciążenie statyczne półki wynosi nawet 100kg.
- Półka wykonana ze stali walcowanej na zimno o grubości min 1,8mm.
- Malowana proszkowo na kolor czarny RAL9004.
- Regulowane tylne uchwyty montażowe.
- Perforowana płyta pozioma. Maksymalny rozstaw uchwytów 550mm.
- 4 punkty montażu

Panel wentylacyjkny z termostatem

- Wentylator dachowy 4 wiatrakowy z termostatem przeznaczony do montażu w szafach stojących o głębokości 800mm.
- Obudowa wykonana z blachy walcowanej na zimno o grubości 1,1mm i malowana proszkowo na kolor czarny RAL9005.
- Wbudowany termostat o płynnej regulacji w zakresie 0-60 °C.
- Wbudowane gniazdo zasilające typu IEC męskie (zasilanie 230V).
- Pobór prądu zespołu wentylacyjnego 0,30A.
- Wydajność wentylatorów (min/max) 660/796 m3/h.
- Liczba obrotów na minutę pojedynczego wentylatora (min/max) 2800/3000 obr/min.
- Poziom hałasu całego zespołu wentylacyjnego 46 dB.
- Wirnik wentylatora jest umieszczony na łożyskach kulkowych.
- Obudowa pojedyńczego wentylatora wykonana z aluminium i malowana proszkowo na kolor czarny.
- W zestawie kabel zasilający o długości 1,8m

Mikrofon przewodowy stołowy

Mikrofon z gęsią szyjką o konstrukcji modułowej z możliwością wymiany przetwornika mikrofonowego na podstawie z włącznikiem.

- rodzaj przetwornika mikrofonowego: pojemnościowy
- charakterystyka kierunkowości: kardioidalna
- pasmo przenoszenia m.cz.: 40 ÷ 20 000 Hz
- skuteczność w polu swobodnym: ≥ 10 mV/Pa

- zastępczy poziom szumów: ≤ 26 dBA.
- średnica przetwornika mikrofonowego: ≤ 12 mm
- długość szyjki mikrofonowej: 400 ÷ 450 mm
- średnica szyjki mikrofonowej: ≤ 8 mm
- rodzaj obudowy: metalowa z dwoma odcinkami giętkimi – przy złączu i przy przetworniku mikrofonowym
- z pierścieniem świecącym przy aktywnym mikrofonie
- zasilanie: fantom 48 V
- typ złącza: XLR 5-M

Pulpit stołowy z wyłącznikiem do mikrofonu z gęsią szyjką z pierścieniem świecącym.

- rodzaj obudowy: metalowa
- masa: 1000 ÷ 1500 g
- typ złączy: XLR 5
- zasilanie: fantom 48 V
- rodzaj wyłącznika przyciskowy z dwukolorowym podświetleniem sygnalizującym stan aktywności mikrofonu:
- kolor zielony – mikrofon włączony, kolor czerwony – mikrofon wyłączony

Aktywny splitter antenowy

Do rozdzielenia sygnału antenowego z dwóch anten odbiorczych na cztery odbiorniki pracujące w systemie odbioru różnicowego.

- zakres częstotliwości transmisyjnych: UHF, zgodny z odbiornikami
- ilość wejść sygnałowych w.cz. 2 – dla systemu z odbiorem różnicowym
- ilość wyjść sygnałowych w.cz. ≥ 4 pary - dla podłączenia nie mniej niż 4 odbiorników z systemu odbioru różnicowego
- wzmocnienie/tłumienie sygnału 0 dB (± 1 dB)
- typ złączy antenowych: BNC
- rodzaj obudowy: metalowa, montowalna w panel 1U, 19”
- wyposażenie splitera: 8 kabli antenowych do połączenia wyjść antenowych splitera z wejściami antenowymi odbiorników

Anteny zewnętrzne

Pasywna antena wielokierunkowa. Nadawanie i odbiór sygnałów w zakresie częstotliwości od 450 do 960 MHz. Zgodna z zaoferowanymi mikrofonami i splitterem antenowym.

Stacja dokująco-ładująca

Stacja dokująco ładująca dla 2 mikrofonów bezprzewodowych do ręki bez wyciągania akumulatorów, zasilacz, 2 szt akumulatorów. Ładowarka zgodna z oferowanymi mikrofonami bezprzewodowymi.

4.1.14 Instalacja audio-wizualna dziedzińca

Przedmiotem opracowania jest projekt wykonawczy wyposażenia multimedialnego oraz oświetlenia scenicznego dla dziedzińca szpitalnego.

W skład opracowania wchodzą następujące systemy:

- system prezentacji obrazów,
- system nagłośnienia,
- system zintegrowanego sterowania AV i transmisji sygnałowej,
- system zarządzania urządzeniami AV,
- system zarządzania wyposażeniem multimedialnym,
- system oświetlenia scenicznego (wg projektu elektrycznego).

Założenia programowe i funkcjonalne

Główne założenia programowe i funkcjonalne:

- wyświetlanie prezentacji multimedialnych,
- nagłośnienie prezentacji multimedialnych,
- sterowanie wyposażeniem multimedialnym,
- sterowanie oświetleniem scenicznym,
- sterowanie oświetleniem DALI,
- nagłośnienie małych koncertów,
- nagłośnienie występów.

System Zarządzania powinien umożliwiać kompleksowe zarządzanie wszystkimi systemami składowymi:

- prowadzenie konferencji, prezentacji multimedialnych, szkoleń itp.,
- łatwość obsługi i automatyka dostosowania systemów zgodnie z wymogami Użytkownika,
- oferowanie rozwiązań praktycznie zweryfikowanych w realizacjach podobnych obiektów o wysokim standardzie wyposażenia,
- możliwość nadzoru i zarządzania wyposażeniem multimedialnym,
- wymagana jest spójność i wysoka niezawodność systemu dlatego system dystrybucji sygnałów AV wraz z systemem sterowania ma być jednego producenta.

Nagłośnienie oraz oświetlenie przystosowane do zarządzania przez technika. Przyłącza do podpięcia urządzeń zarządzających zlokalizowane we floorboxie w rogu sali.

Dziedziniec – system wizyjny

W pomieszczeniu zostaną zainstalowane wysokiej klasy 4 monitory 55” (VideoWall) w zabudowie ściennej na dedykowanej konstrukcji umożliwiającej dostęp techniczny indywidualnie do każdego monitora. Na monitorach po podłączeniu się urządzeniami źródłowymi do zainstalowanych przyłączy AV będzie można wyświetlać dowolne obrazy.

Przyłącza AV wyposażone w przyłącza VGA audio oraz HDMI zostały zlokalizowane w 3 miejscach, tj. ściana pod panele dotykowym, w podeście, w szafce mobilnej. Wszystkie sygnały są transmitowane do szafy rack zlokalizowanej w pomieszczeniu technicznym w formie cyfrowej poprzez okablowanie CAT6 w ekranie, gdzie trafiają do switchera HDMI, a następnie dalej w formie cyfrowej do ściany Videowall.

Dziedziniec – system audio

System nagłośnienia ma za zadanie wspomagać elektroakustycznie małe formy muzyczne, konferencje itp. odbywające się na projektowanym dziedzińcu. System głośnikowy ma charakteryzować się:

- Bardzo wysoka jakość dźwięku systemu oferująca pasmo zestawów szerokopasmowych minimum 80Hz – 20KHz (-3dB) oraz niskotonowych pracujących od minimum 30Hz (-6dB)

- Ze względu na specyfikę pomieszczenie i powierzchnie silnie odbijające na suficie i podłodze należy zaprojektować system oparty na urządzeniach głośnikowych wykorzystujących technologię wyrównaną liniowo z możliwie małym kątem zasięgu w pionie oraz z możliwością modelowania lub budowania klastrów tak aby uzyskać niesymetryczną propagację w poziomie (minimalizująca odbicia od ścian).
- System ma uzyskać poziom dźwięku minimum 110 dB z nierównomiernością ≤ ±3dB na minimum 90% powierzchni odsłuchowej.

System powinien bazować na cyfrowej transmisji sygnału dźwięku od wejść mikser audio po wyjścia wmacniaczy. System ma zapewnić dźwięk wyrównany w widmie tak że dla zakresów niskich tonów (Low), średnich (Mid) oraz wysokich (High) nierównomierność nie jest gorsza niż ≤ ±2dB. System musi być gotowe na przyjęcie i miksowanie co najmniej 24 kanałów audio. System musi być wyposażony w wielofunkcyjne monitory sceniczne.

Na wyposażeniu znajdą się 3 wysokiej klasy mikrofony bezprzewodowe dwa do ręki oraz jeden nagłowny. Ponadto zaprojektowano wysokiej kasy mikrofony przewodowe z przyłączami w podeście scenicznym. W celu zapewnienia wysokiej jakości odbioru sygnału z mikrofonów bezprzewodowych zaprojektowano zewnętrzne anteny odbiorcze.

W szafie rack znajdzie się player audio oraz Blu ray umożliwiając tym samym odtwarzanie muzyki oraz wyświetlanie materiałów z płyt Blu ray. Dodatkowo został zaprojektowany drugi player audio w szafie mobilnej.

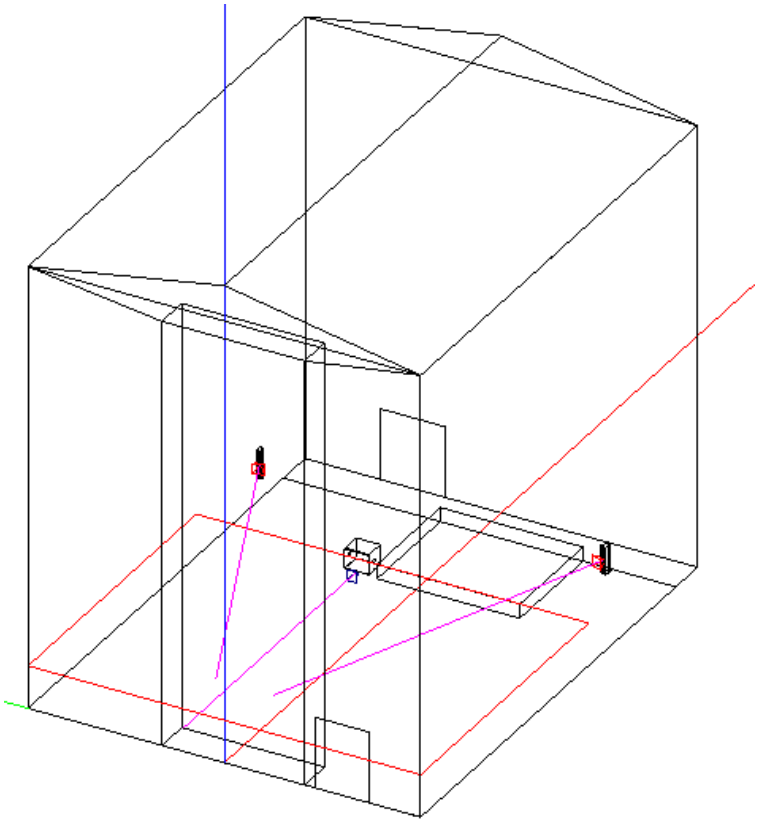
<u>Dziedziniec – system sterowania</u>

Zaprojektowano system sterowania umożliwiając zarzadzanie systemami audio video oraz oświetlenia użytkowego i scenicznego za pomocą:

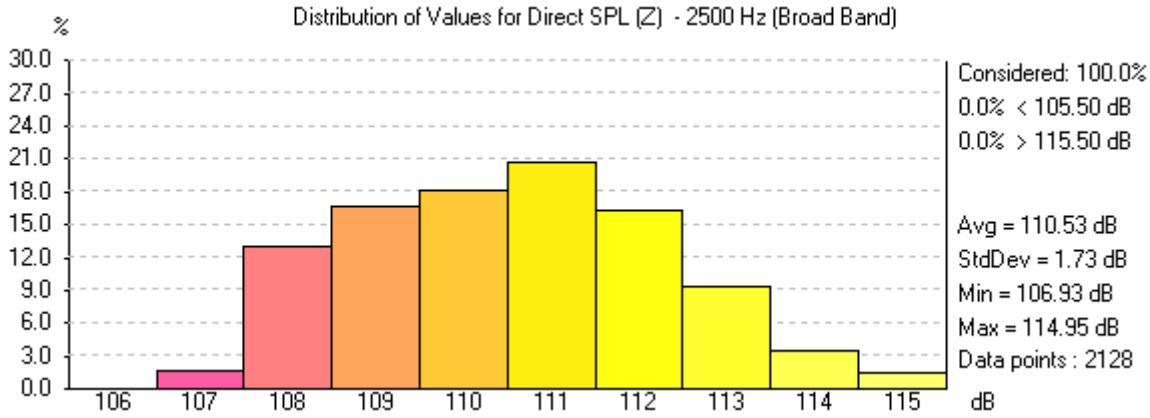
- panel dotykowego 5” zabudowanego w przedniej ścianie nad przyłączem AV- niezbędne funkcje do codziennego użytku,
- klawiatury przy drzwiach –sterowanie oświetleniem,
- bezprzewodowy panel dotykowy – rozbudowany system sterowania do obsługi przez osoby technicznie przeszkolone,
- komputera z oprogramowaniem do sterowania DMX.

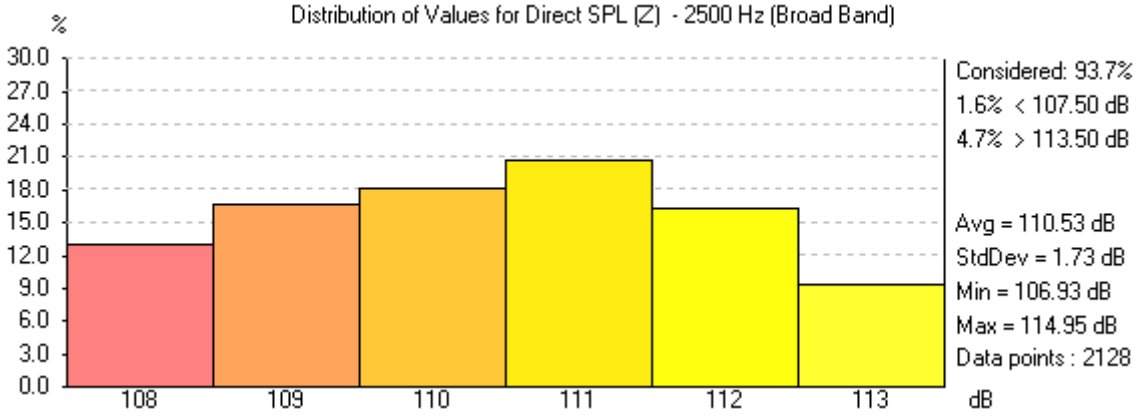
<u>Dziedziniec – symulacje akustyczne</u>

Symulacje akustyczne wykonano w programie symulacyjnym EASE 4.1.

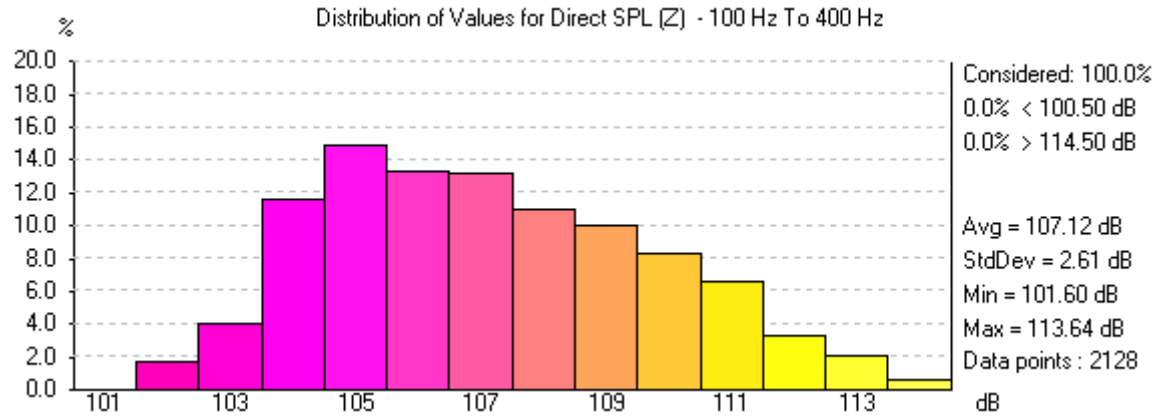


Poziom dźwięku bezpośredniego 100Hz – 10KHz

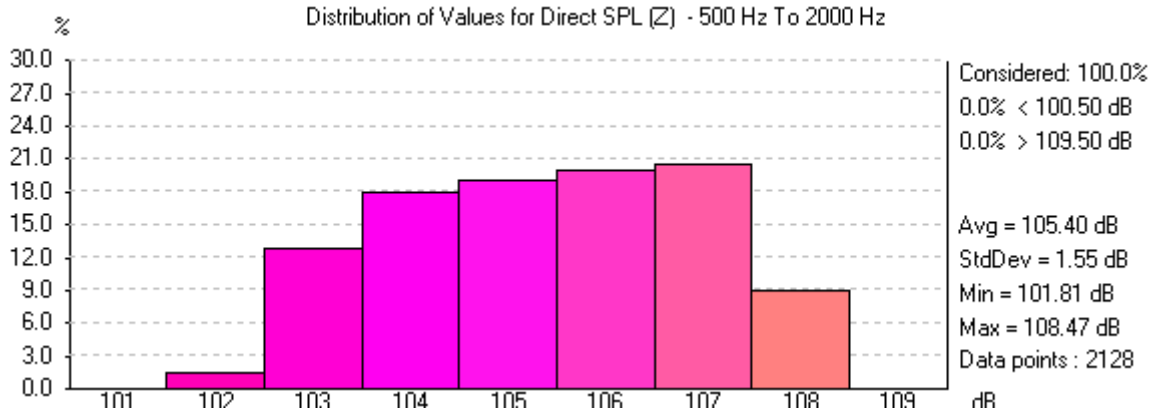

Distribution of Values for Direct SPL (Z) - 2500 Hz (Broad Band)
%
30.0
27.0
24.0
21.0
18.0
15.0
12.0
9.0
6.0
3.0
0.0
106
107
108
109
110
111
112
113
114
115
dB
Considered: 100.0%
0.0% < 105.50 dB
0.0% > 115.50 dB
Avg = 110.53 dB
StdDev = 1.73 dB
Min = 106.93 dB
Max = 114.95 dB
Data points : 2128


Distribution of Values for Direct SPL (Z) - 2500 Hz (Broad Band)
%
30.0
27.0
24.0
21.0
18.0
15.0
12.0
9.0
6.0
3.0
0.0
108
109
110
111
112
113
dB
Considered: 93.7%
1.6% < 107.50 dB
4.7% > 113.50 dB
Avg = 110.53 dB
StdDev = 1.73 dB
Min = 106.93 dB
Max = 114.95 dB
Data points : 2128

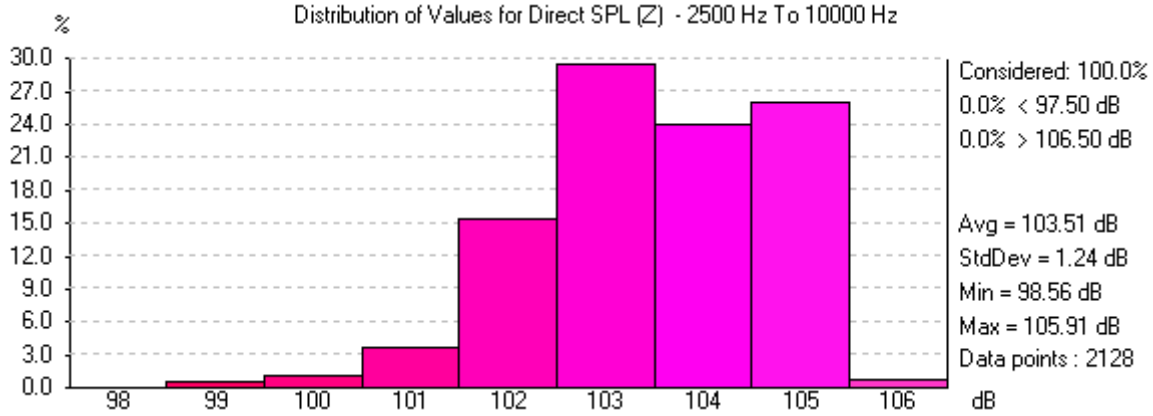
Poziom dźwięku bezpośredniego dla pasma 100Hz-400Hz



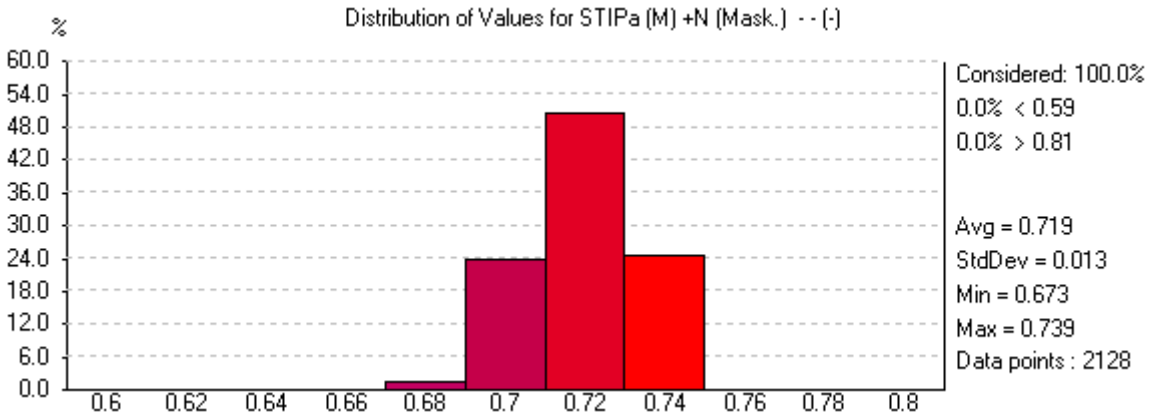
Poziom dźwięku bezpośredniego dla pasma 500Hz-2000Hz



Poziom dźwięku bezpośredniego dla pasma 2500Hz-10 000Hz



Zrozumiałość mowy STIPa



Podsumowanie obliczeń:

Lp.	Parametr	Wartość	Nierównomierność	Uwagi
1	Poziom dźwięku bezpośredniego w pasmie 100Hz–10 000Hz	110,5 dB	+/-3dB na 94%	
2	Poziom dźwięku bezpośredniego w pasmie 100Hz-400Hz	107,1 dB	+/- 1,8dB	
3	Poziom dźwięku bezpośredniego w pasmie 500Hz-2 000Hz	105,4dB		
4	Poziom dźwięku bezpośredniego w pasmie 2500 Hz-10 000Hz	103,5dB		
5	Zrozumiałość mowy STIPa	0,72		Uwzględnione maskowanie sygnału oraz tło akustyczne.

Elementy systemu oraz pozostałe informacje

Elementem sterującym będą panele dotykowe oraz klawiatury sterujące. W pamięci jednostki centralnej w trakcie instalowania i programowania systemu zapisane będą programy wykonawcze. Programy te, definiujące funkcje poszczególnych okien i przycisków panelu dotykowego sterują funkcjami poszczególnych urządzeń oraz wykonują MAKROPROGRAMY - sekwencje instrukcji uruchamianych po naciśnięciu jednego klawisza – np. LAPTOP spowoduje włączenie Videowall i odpowiedniego źródła, zatrzymanie innych źródeł, ustawienie wymaganego poziomu głośności prezentacji multimedialnych oraz np. odpowiednie oświetlenie sali.

Przyłącze aktywne w danym momencie, będzie posiadać swoje odzwierciedlenie na panelach sterujących odpowiednią sygnalizacją.

Harmonogram czasowy włączania i wyłączania systemu, np. system aktywny od godz 6:00 wyłączenie systemu godz 22:00.

Projekt i specyfikacja projektowa są kompletne z punktu widzenia celu, któremu mają służyć.

Opis funkcjonalny, minimalne parametry urządzeń, schematy blokowe, rzuty rozmieszczenia urządzeń, tworzą zbiór minimalnych wymagań stawianych systemowi dla projektowanego obiektu i należy traktować je jako spójną całość.

Projektant stanowi nadzór autorski nad realizacją całego projektu. Wszelkie zmiany w projekcie i specyfikacji mogą być wprowadzone tylko za jego pisemną zgodą.

Minimalne parametry urządzeń

Monitor do ścian wizyjnych 55”

- Panel IPS
- Min. przekątna ekranu 55”
- Rozdzielczość: 1920 x 1080 (FHD)
- Proporcje obrazu: 16:9

- Min. jasność: 700 cd/m2
- Czas działania: 24/7
- Min. czas reakcji: 8 ms
- Grubość ramki: 0,9 mm
- Poziom kontrastowości statycznej: 1400:1
- Kąt widzenia: 178 o x 178 o
- Waga: nie więcej niż 27 kg
- Wejścia: HDMI, Display Port, Rj45 (LAN)
- Dodatkowo: LAN Daisy Chain zarządzanie przez LAN

Zestaw 4 monitorów na uchwytach tworzący ścianę monitorów (tzw. "VideoWall") wspólnie sterowaną i posiadającą oprogramowanie dopasowujące balas bieli, jasność, kontrastować poszczególnych monitorów w taki sposób, aby połączone monitory wyglądały jak jeden obraz bez różnic w jasności na połączeniach monitorów.

Konstrukcja Video wall

Konstrukcja umożliwiająca zainstalowanie 4 monitorów tworząć we wnęce ściankę 2x2. Niezależna, 8-pozycyjna regulacja pozwala na precyzyjne wyrównanie ekranów bez konieczności używania narzędzi.

Mechanizm wysuwny zapewnia wygodny dostęp serwisowy do ekranów instalowanych we wnękach i miejscach z utrudnionym dostępem serwisowym.

Otwarta konstrukcja produktu daje pełny dostęp do okablowania, a zawarte w zestawie opaski ułatwiają organizację kabli. Zakres regulacji każdego ekranu w zakresie min 100-260mm.

Nadajnik sygnałowy PAV 1 ścienny

Nadajnik ścienny do montażu podtynkowego z wbudowanym switcherem, auto detekcja podłączonego źródła, wbudowany scaler sygnałowy, wejście HDMI, VGA audio, Ethernet.

Odbiornik posiadający wejście HDMI, wyjście HDMI, wyjście audio, RS232, IR, Ethernet.

Transmisja na min 70m.

Nadajnik sygnałowy PAV 2 ścienny

Nadajnik ścienny do montażu podtynkowego z wbudowanym switcherem, auto detekcja podłączonego źródła, wbudowany scaler sygnałowy, wejście HDMI, VGA audio, Ethernet.

Odbiornik posiadający wejście HDMI, wyjście HDMI, wyjście audio, RS232, IR, Ethernet.

Transmisja na min 70m.

Nadajnik sygnałowy floorbox

Nadajnik kompaktowy z wbudowanym switcherem, auto detekcja podłączonego źródła, wbudowany scaler sygnałowy, 2 xwejście HDMI, VGA audio w nadajniku.

Odbiornik posiadający wejście HDMI, wyjście HDMI, wyjście audio, RS232, IR, Ethernet.

Transmisja na min 70m.

Wypełnienie floorboxa dla technika

Wypełnienie wg planowanego wyposażenia zgodnie z schematem blokowym.

Wypełnienie PP2

Wypełnienie wg planowanego wyposażenia zgodnie z schematem blokowym.

Wypełnienie XLR

Wypełnienie floorboxa: 16 złącz XLR

Odbiorniki transmisji AV 1

Odbiornik cyfrowego sygnału HDBaseT, wyjście HDMI, wbudowany scaler video obsługujący rozdzielczości do 4K/60 włącznie, port dwukierunkowy RS-232, IR, Ethernet, USB HID. Deembeder audio, HDCP 2.2.

Switcher Video audio

Przełącznik z wbudowanym scalerem sygnałowym obsługujący także rozdzielczosci 4K. 4 x wejscie VGA audio, 4 x HDMI, wyjście HDMI, wyjście HDBaseT, wyjście audio, MIC, RS232, LAN, 2x USB.

Blue Ray RS232

Uniwersalny odtwarzacz audio – video; odtwarzanie BlueRay, DVD, CD, nośniki USB, obsługa DLNA 1.5.

- Odtwarzane typy plików: Dekodowanie: Video | DivX 3, 4, 5, 6; DivX HD; MPEG-1; MPEG-2; MPEG-4; MPEG-4 AVC (H.264); VC-1 (Windows Media Video); Xvid, Dekodowanie audio: AAC; Dolby Digital; Dolby Digital Plus; Dolby TrueHD; DTS Digital Surround; DTS-HD; WMA; obsługiwane formaty USB: FAT16, FAT32, NTFS; obsługiwane pamięci / dyski USB o pojem¬ności do 2TB (minimum).
- Parametry audio: Minimalne pasmo przenoszenia: 20Hz 20kHz (+0,5dB); Odstęp od szumów > 100 dB (A); zakres dynamiki (nie gorszy niż) 100 dB (A); zniekształcenia (nie większe niż) 0,05%; separacja kanałów (lepsza niż) 90 dB.
- Złącza:Wyjście HDMI;analogowe wyjście audio stereo symetryczne (XLR) i niesymetryczne; cyfrowe wyjście audio; gniazdo USB; złącze Ethernet;złącze RS232.
- Sterowanie: Pilot IR;LAN;RS232.
- Przystosowany do montażu w szafie RACK (wysokość maksymalna 1U).

Kabel HDMI 2m

- Złącza HDMI-HDMI, męsko-męskie
- Obsługa rozdzielczości do 4K * 2K@60Hz
- Wysoko elastyczny przewód
- Obsługa ARC, 3D, HDCP, CEC
- Zawartość miedzi w przewodzie min. 99,99%
- Potrójnie ekranowany przewód
- Pozłacane złącza
- Długość przewodu - 2m

Mikrofon bezprzewodowy do ręki

Nadajnik:

- zakres częstotliwości transmisyjnych: UHF zgodny z odbiornikiem
- zakres zmian częstotliwości transmisyjnej: > 40 MHz
- skok przestrajania: 25 kHz
- moc wyjściowa w.cz.: ≥ 30 mW
- rodzaj przetwornika mikrofonowego: dynamiczny kardioidalny
- maksymalny poziom wysterowania: 154 dB SPL
- pasmo przenoszenia m.cz.: 80÷18 000 Hz
- zakres zmian czułości wejściowej nadajnika: 40 dB
- tryb przełączania czułości wejściowej: skokowo, skok ≤ 6 dB
- zniekształcenia nieliniowe: < 1 %

- stosunek sygnał/szum: 110 dB(A)
- wyświetlacz ze wskazaniem: częstotliwości transmisyjnej
- poziomu wysterowania audio
- stanu naładowania ogniw zasilających
- port podczerwieni do synchronizacji z odbiornikiem: częstotliwości transmisyjnej
- zasilanie: 2 ogniwa AA
- czas pracy z 1 kompletu ogniw ≥ 8 h
- rodzaj obudowy: metalowa

Odbiornik:

- system odbioru: dwu-antenowy różnicowy „true diversity”
- zakres częstotliwości transmisyjnych: UHF
- zakres zmian częstotliwości transmisyjnej: > 40 MHz
- skok przestrajania: 25 kHz
- pasmo przenoszenia m.cz.: 25 ÷ 18 000 Hz.
- zniekształcenia nieliniowe: ≤ 1 %
- stosunek sygnał/szum: ≥ 110 dB(A)
- typ złącza wyjściowego sygnału audio, standard sygnału : XLR, sygnał symetryczny
- poziom sygnału wyjściowego przy dewiacji nominalnej: ≥ 12 dBu
- wyświetlacz ze wskazaniem: częstotliwości transmisyjnej
- poziomu sygnału antenowego
- poziomu wysterowania audio
- stanu naładowania ogniw nadajnika
- skanowanie pasma z wyszukiwaniem niezakłóconych częstotliwości transmisyjnych
- port podczerwieni do synchronizacji z nadajnikiem: częstotliwości transmisyjnej
- typ złączy antenowych: BNC
- rodzaj obudowy: metalowa, montowalna w panel 1U, 19”

Mikrofon bezprzewodowy nagłowny

Zestaw bezprzewodowy z mikrofonem nagłownym

Wszystkie urządzenia pracują w układzie "diversity" zapewniając ciągłość transmisji, posiadają metalowe obudowy szerokości 1/2 rack, ciekłokrystaliczne wyświetlacze , wskaźnik stanu baterii.

- Praca w paśmie UHF (516 MHz-865 MHz)
- 6 wersji częstotliwościowych
- Szerokość pasma roboczego: 42 MHz
- Liczba częstotliwości nośnych: maks. 1680
- 12 banków ze stałymi częstotliwościami (preset)
- Programowanie nadajników w stanie nieaktywnym (Silent Configuration Mode).
- Rozszerzony zakres regulacji czułości wejściowej nadajników
- Equalizer
- Układ redukcji szumów i zwiększania dynamiki HDX.
- Funkcja Sync: do bezprzewodowego przekazu z odbiornika do nadajnika częstotliwości, nazwy i sygnału pilotującego.
- Pasmo przenoszenia: 80 Hz - 18 kHz

- Dewiacja: +/- 48 kHz
- Stosunek sygnał/szum: >110 dB
- Moc nadajnika: 30 mW
- Sygnalizacja wyczerpania baterii w nadajniku i odbiorniku.
- Wyjście sygnału symetryczne: jack stereo, XLR
- Anteny montowane do gniazd BNC 50 Ohm
- Zewnętrzne styki do ładowania akumulatora w nadajniku (prócz SKP)
- Funkcja Mute: wyciszenie nadajnika
- Blokada przycisków funkcyjnych przed przypadkowym naciśnięciem
- Zasilanie nadajników: 2 x ogniwoAA

Mikrofon przewodowy

Mikrofon przewodowy, przetwornik dynamiczny, charakterystyka super-kardioidalna, pasmo-przenoszenia 40-16000 Hz.

Dystrybutor antenowy z zasilaczem

Do rozdzielenia sygnału antenowego z dwóch anten odbiorczych na cztery odbiorniki pracujące w systemie odbioru różnicowego.

- zakres częstotliwości transmisyjnych: UHF, zgodny z odbiornikami
- ilość wejść sygnałowych w.cz. 2 – dla systemu z odbiorem różnicowym
- ilość wyjść sygnałowych w.cz. ≥ 4 pary - dla podłączenia nie mniej niż 4 odbiorników z systemu odbioru różnicowego
- wzmocnienie/tłumienie sygnału: 0 dB (± 1 dB)
- typ złączy antenowych: BNC
- rodzaj obudowy: metalowa, montowalna w panel 1U, 19”
- wyposażenie splitera: 8 kabli antenowych do połączenia wyjść antenowych splitera z wejściami antenowymi odbiorników

Antena zewnętrzna

Pasywna antena wielokierunkowa. Nadawanie i odbiór sygnałów w zakresie częstotliwości od 450 do 960 MHz. Zgodna z zaoferowanymi mikrofonami i splitterem antenowym.

Uchwyt ścienny do anteny

Uchwyt umożliwiający montaż anteny mikrofonowej do ściany.

Uchwyt RACK do odbiorników mikrofonu

Uchwyty do zamontowania 2 odbiorników mikrofonowych w panel 1U, 19”.

Statyw mikrofonowy wysoki

Statyw do mikrofonu

- wysokość w zakresie min 100cm do 230cm, nóżki min 30cm, zakończone nasadką gumową, ramię poziome min 70cm, zakończone gwintem 3,8", podstawa składana, waga w zakresie 3-5 kg
- Wykonanie: rury cienkościenne stalowe, lakier proszkowy czarny półmatowy, wszystkie elementy konstrukcyjne wykonane metodą wtrysku ciśnieniowego, pokrętła plastikowe wykonane z wysokoudarowego poliamidu

Statyw mikrofonowy niski

Statyw do mikrofonu (niski). Wykonanie rury cienkościenne stalowe precyzyjne, lakier proszkowy czarny półmatowy, wszystkie elementy konstrukcyjne wykonane metodą wtrysku ciśnieniowego, pokrętła plastikowe wykonane z wysokoudarowego poliamidu.

- Wysokość w zakresie min 70-150 cm
- Wysięgnik teleskopowy poziomy, zakończony gwintem 3/8"
- Nóżki min 30 cm zakończone nasadką gumową z regulowaną średnicą rozstawu

Player audio

Odtwarzacz CD w obudowie rack 19 cali 1U, napęd bezszczotkowy. Wyszukiwanie indeksów dla płyt audio CD. Określenie czasu przerw między ścieżkami. Niesymetryczne analogowe wyjścia RCA. Cyfrowe wyjście optyczne (SPDIF).

Współosiowe wyjście cyfrowe (SPDIF). Wyjście mono. Złącze szeregowe (RS-232C, D-sub, 9-pin), wyjście słuchawek z gałką poziomu głośności.

Podświetlany ekran LCD. Dołączony bezprzewodowy pilot zdalnego sterownia (możliwość wyłączenia odbiornika sygnału).

Procesor audio

- 12 wejść analogowych (z zasilaniem Phantom 48v w każdym kanale)
- 8 wyjść analogowych
- Konfigurowalne przetwarzanie audio
- Bogata paleta obiektów przetwarzania i logicznych
- 48-kanałowa, niskolatencyjna, odporna na błędy, cyfrowa szyna audio
- Przejrzysta sygnalizacja LED na panelu przednim
- Funkcja dwukierunkowej lokalizacji
- 12 wejść sterujących i 6 wyjść logicznych, umożliwiających integrację z GPIO

Bramka Dante do procesora audio - ekspander

Bramka Dante do procesora audio-expander. Wyposażona w RS232 oraz ethernet. Do współpracy z oferowanym procesorem audio.

Kolumna ścienna

Dwudrożna kolumna głośnikowa wykorzystująca technologię źródeł wyrównanych liniowo. Niesymetryczna propagacja w poziomie: 30° - 60°. Propagacja w pionie 12°. Odpowiedź częstotliwościowa 80Hz - 20KHz (-3dB). Moc znamionowa: 700W. Efektywność 97dB. Poziom maksymalny 131dB. Budowa: LF 4 x 5", HF: 2 x 4" przetwornik fali płaskiej. Waga <16kg.

Zestaw hornów

Zestaw hornów do dokonywania modyfikacji w płaszczyźnie pionowej dla 60° lub 90° (30°+60° or 60°+30°).

Uchwyt ścienny kolumny

Uchwyt ścienny umożliwiający zwieszenie ramy do kolumny, zdystansowanie od ściany zgodnie z projektem architektury.

Wzmacniacz mocy DSP

Wzmacniacz mocy 4 x 1250W/RMS/2Ohm (4 x 2800W peak). Wejscia analogowe, AES3, sieć cyfrowa. Procesor DSP. Presety dla wykorzystanych urządzeń głośnikowych. Zarżadzalne w dedykowanym interfejsie na komputerze typu PC.

Subwoofer

Urządzenie niskotonowe. Przetwornik 1 x 18" neodymowe. Odpowiedź częstotliwościowa (-6dB): 30Hz - 120Hz. Moc AES: 1250W. Skuteczność 1W/1m: 102dB. Poziom maksymalny 139dB.

Monitor sceniczny wielofunkcyjny

Aktywny monitor wielofunkcyjny wyposażony w 12” przetwornik współosiowy, 520W mocy, Max. SPL 128 dB, wbudowany procesor DSP z wyświetlaczem LCD, 5 presetów fabrycznych / presetów użytkownika, Delay line, EQ, filtr Low-Cut.

Floorbox monitor sceniczny 1 i 2

Wyposażenie floorboxa dedykowane dla monitora scenicznego (odsłuch).

Cyfrowy mikser

24 kanałowy cyfrowy mikser z 7" ekranem dotykowym LCD. 16 wejść mikrofonowo liniowych, 8 wejść typu Insert. 4 wejścia liniowe TRS, 4 wejścia liniowe RCA. 8 wysylek typu AUX (lub 4 x Aux + 4 x podgrupa). 6 grup DCA. Jeden zmotoryzowany fader Alps, 100mm przypisywany plynnie do wybranych wejść. Wejście USB 2 kanałowe. 4 wyjścia AUX i 4 wyjśca podgrup. Zaawansowany procesor DSP (kompresor, limiter, ekspander, bramka, EQ i inne) oraz wbudowany procesor efektów. Interface Dante. Kontrola i sterowanie z urządzeń typu IPAD. Zakres dynamiki min 106dB. Częstotliwość próbkowania 48KHz, rozdzielczość 32 bity. Interfejs Dante.

Jednostka centralna

Jednostka centralna systemu sterowania z możliwością zamontowania w racku. Komunikacja poprzez ethernet, okablowanie magistralne, RS232, IR. 8x RELAY, 8 x port I/O, 3 x COM, slot pamięci SD, obsługa do 10 programów jednocześnie, procesor umożliwia wykonanie wirtualne panela sterowania na dowolny komputer, tablet.

Panel sterujący 5”

5" ekran dotykowy TFT zasilany POE zamontowany na ścianie do puszki montażowej podtynkowej wyposażony dodatkowo w pięć przycisków, wbudowany mikrofon, wbudowany głośnik, obsługa formatu H.264, jasność min 400 cd, 5 punktowy multitouch, intercom, wyświetlanie strumieniowanego obrazu wideo. Panel montowany na podtynkowej puszce.

Zasilacz PoE

- Zgodne ze standardem 802.3af oraz 802.3at
- Port wejścia RJ-45 1000 Mb/s
- Port wyjścia danych oraz zasilacza 1000 Mb/s

Klawiatura sterująca ścienna

Możliwe konfiguracje przycisków: 4, 6.

- 1x złącze magistrali systemowej
- Zintegrowany fotosensor
- 2x wejście cyfrowe
- Zasilanie poprzez magistralę systemową

- W zestawie z klawiaturą: 2x paski przycisków średnich (po 3 przyciski), 2x paski przycisków dużych (po 2 przyciski)
- Kolor biały lub czarny

Sterownik oświetlenia DALI

Dwukanałowy ściemniacz do sterowania balastami opraw

- Maksymalna ilość balastów– 128
- Ilość kanałów ściemniacza: 2
- 2x Port magistrali komunikacyjnej
- 2x porty override
- Port USB typu B
- Wyświetlacz informujący o numerze identyfikacyjnym urządzenia
- Konfiguracja poprzez panel frontowy lub oprogramowanie
- Wskaźniki LED
- Przycisk resetujący wewnętrzny procesor
- Moduł przystosowany do montażu na szynie DIN, szerokość 9 modułów

Router

- Procesor: min 2 rdzenie, min 1.4 GHz
- 10 gigabitowych portów Ethernet
- 1 port SFP;
- 1 port USB 3.0;
- dotykowy ekran;
- wyjście PoE;
- możliwość montażu w szafie RACK;
- monitorowanie napięcia;

Access point

- Port LAN: 10/100/1000Mb/s
- Transfer danych: 867 Mb/s
- Częstotliwość: 2,4 GHz i 5 GHz
- Zakres: min. 180 m
- Szyfrowanie: AES,TKIP,WEP,WPA,WPA-PSK,WPA2

Bezprzewodowy panel dotykowy z aplikacją

Przekątna ekranu 9,7 cala. Ekran o rozdzielczości 2048x1536. Powłoka oleofobowa odporna na odciski palców. Zdjęcia o rozdzielczości 5 mln pikseli. Nagrywanie wideo w rozdzielczości HD. Pamięć Flash 16GB Procesor A7 i 64 bitowa architektura. Wytrzymałość baterii do 10 godzin. Czujnik oświetlenia w otoczeniu. Aplikacja umożliwiająca wykonanie programu do zarządzania systemem AV (zgodna z systemem sterowania).

Bramka DMX

Dwukierunkowy interfejs do komunikacji DMX RS232. Obsługa do 512 kanałów.

Zasilacz systemowy na szynę DIN

6 portów magistrali systemowej.

- Montaż na szynie DIN
- Moc wyjściowa 60W.
- Pobór mocy 70W.
- Możliwości montażowe: montaż na szynie DIN, szerokość 6 modułów DIN.

Moduł przekaźnikowy

- Ilość przekaźników (kanałów): 8.
- Maksymalne obciążenie dla opraw świetlówkowych na kanał: 5A.
- Maksymalne obciążenie dla opraw żarowych na kanał: 10A.
- Maksymalne obciążenie rezystancyjne: 16A.
- 2 porty override.
- Port magistrali komunikacyjnej kompatybilny z innymi urządzenia systemu sterowania.
- Przystosowany do pracy 230V/50Hz.
- Zasilanie: 24V DC poprzez port magistralowy.
- Konfiguracja poprzez panel frontowy lub oprogramowanie.
- Wskaźniki LED informujące o: komunikacji, zasilaniu, trybie override, statusie każdego kanału.
- Wyświetlacz numeryczny wskazujący numer identyfikacji w sieci.
- Przycisk resetujący wewnętrzny procesor.
- Możliwości montażowe: montaż na szynie DIN, szerokość 9 modułów DIN.

Kabel HDMI 5m

- Złącza HDMI-HDMI, męsko-męskie
- Obsługa rozdzielczości do 4K * 2K@60Hz
- Wysoko elastyczny przewód
- Obsługa ARC, 3D, HDCP, CEC
- Zawartość miedzi w przewodzie min. 99,99%
- Potrójnie ekranowany przewód
- Pozłacane złącza
- Długość przewodu - 5m

Kabel VGA+audio 5m

- Złącza VGA/Audio-VGA/Audio, męsko-męskie
- Przewód VGA z zintegrowanym przewodem audio 3,5 mm
- Obsługa rozdzielczości do 1920*1200
- Wysoko elastyczny przewód
- Potrójnie ekranowany przewód
- Długość przewodu - 5m

Szafka RACK mobilna

- Profesjonalna skrzynia na urządzenia 482mm (19"), z kółkami i 2 blatami
- Funkcjonalna konstrukcja umożliwia bezpieczny transport, szybki montaż i demontaż.

- Przestrzeń montażowa 9U na urządzenia obsługiwane od góry (np. miksery); możliwość nachylenia
- Przestrzeń 16U dla urządzeń wymagających pozycji poziomej
- Przeznaczona do urządzeń o głębokości max 480mm
- Panele przedni i tylny z rozkładanymi nogami (stołowymi), powierzchnia użytkowa: około 920x525mm, wysokość: około 760mm
- 9mm drewniana sklejka, odporna na wilgoć, laminowana czarnym tworzywem sztucznym
- Stabilna płyta dolna o grubości 13mm
- Aluminiowe profile na krawędziach
- Chromowane narożniki kulowe oraz kątowniki
- Kółka 100mm (2 z blokadą)
- Zamknięcia motylkowe
- 2 uchwyty wpuszczane po obu stronach, zapewniające bezpieczny i wygodny transport
- W komplecie akcesoria montażowe
- 70 nakrętek sprężynkowych
- 70 śrub krzyżakowych M6 x 15mm
- 70 plastikowych podkładek

Półka 19” 1U 450mm w szafce mobilnej

- Półka 19" wzmocniona o wysokości 1U z regulowanymi uchwytami montażowymi charakteryzująca się wysoką wytrzymałością statyczną do 100kg.
- Półka wykonana ze stali walcowanej na zimno o grubości min 1,8mm.
- Malowana proszkowo na kolor czarny RAL9004.
- Regulowane tylne uchwyty montażowe.
- Perforowana płyta pozioma. Maksymalny rozstaw uchwytów 550mm.
- 4 punkty montażu

Szafa 19” stojąca 42U 800/800

- Wysokość 42U.
- Głębokość 800mm.
- Drzwi przednie z szybą z hartowanego szkła oraz zamkiem jednopunktowym.
- Drzwi tylne metalowe z zamkiem.
- Możliwość szybkiego przełożenia drzwi z lewych na prawe.
- Zdejmowane i zamykane na klucz panele boczne.
- Wsporniki do montażu wyposażenia 19" z przodu i z tyłu.
- Przepusty kablowe na górze i dole szafy.
- Profile montażowe ze stali ocynkowanej.
- Maksymalne obciążenie szafy : statyczne-800 kg , dynamiczne-400 kg.
- Możliwość zamontowania wentylatora.

Wykonanie:

- Precyzyjne i solidne wykonanie z wysokiej jakości stali SPCC, rama spawana.
- Grubość blach: 2,0mm profile montażowe, 1,2mm. pozostałe elementy.
- Wymiary: 800x800x2020mm. (szerokość x głębokość x wysokość).

- Kolor: czarny RAL 9004

W zestawie :

- 4 szt. nóżek i 4 szt. kółek.
- 4 komplety kluczy do drzwi.
- Zaślepki do przepustów kablowych.

Półka 19" 1U 450mm

- Półka 19" wzmocniona o wysokości 1U z regulowanymi uchwytami montażowymi charakteryzująca się wysoką wytrzymałością statyczną do 100kg.
- Półka wykonana ze stali walcowanej na zimno o grubości min 1,8mm.
- Malowana proszkowo na kolor czarny RAL9004.
- Regulowane tylne uchwyty montażowe.
- Perforowana płyta pozioma. Maksymalny rozstaw uchwytów 550mm.
- 4 punkty montażu.

Panel wentylacyjny

- Wentylator dachowy 4 wiatrakowy z termostatem przeznaczony do montażu w szafach stojących o głębokości 800mm.
- Obudowa wykonana z blachy walcowanej na zimno o grubości 1,1mm i malowana proszkowo na kolor czarny RAL9005.
- Wbudowany termostat o płynnej regulacji w zakresie 0-60 °C.
- Wbudowane gniazdo zasilające typu IEC męskie (zasilanie 230V).
- Pobór prądu zespołu wentylacyjnego 0,30A.
- Wydajność wentylatorów (min/max) 660/796 m3/h.
- Liczba obrotów na minutę pojedynczego wentylatora (min/max) 2800/3000 obr/min.
- Poziom hałasu całego zespołu wentylacyjnego 46 dB.
- Wirnik wentylatora jest umieszczony na łożyskach kulkowych.
- Obudowa pojedyńczego wentylatora wykonana z aluminium i malowana proszkowo na kolor czarny.
- W zestawie kabel zasilający o długości 1,8m.

4.1.15 System kolejkowy

Opis systemu

System zarządzania kolejkami ma na celu sprawne zarządzanie ruchem pacjentów w obszarach punktu pobrań, SORu, izbie przyjęć planowych, diagnostyki obrazowej, poradni i elektrodiagnostyki. Instalacja systemu powinna zapewnić uporządkowanie kolejności obsługi pacjentów poprzez rejestrację i przydzielenie do odpowiedniej kolejki, kierowanie pacjenta do odpowiednich gabinetów/przychodni z zachowaniem pobranego/wydanego numeru kolejkowego.

Elementy składowe systemu

Projektowany system kolejkowy składa się z:

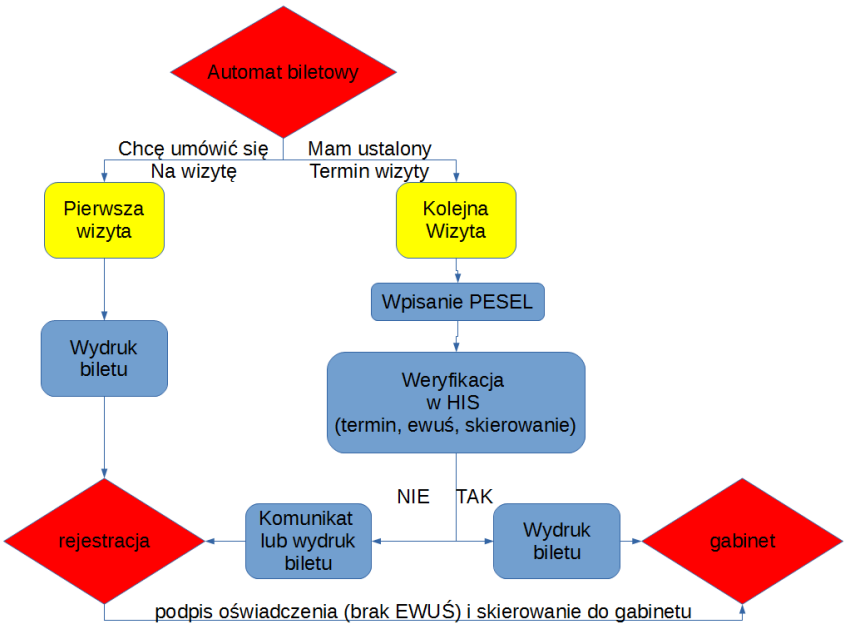
- automatów biletowych, za pomocą których pacjenci będą pobierali bilety z numerkami
- drukarek termicznych do wydawania biletów przez obsługę stanowisk rejestracji
- wyświetlaczy LCD, na których będą prezentowane informacje o aktualnym stanie kolejek i kolejnych przywoływanych pacjentach

- serwera zarządzającego
- oprogramowania.

System musi zapewniać możliwość rozbudowy w przyszłości o kolejne urządzenia.

Przepływ pacjentów

Pacjent zgłasza się do automatu biletowego bądź do strefy rejestracji. Korzystając z systemu kolejkowego dokonuje wyboru celu wizyty lub dokonuje tego za niego obsługa rejestracji. Po otrzymaniu numerku udaje się do odpowiedniego oddziału i oczekuje na wezwanie z systemu kolejkowego. Obrazuje to poniższy graf:



Pacjent w automacie biletowym potwierdza swoją obecność poprzez wpisanie numeru PESEL, dostaje wydrukowany bilet, z którym udaje się do poczekalni oczekując na wezwanie. System sprawdza czy pacjent posiada na dziś umówioną wizytę w systemie medycznym oraz czy ma ważne ubezpieczenie w systemie EWUŚ oraz czy nie jest forsowany do rejestracji (np. w celu dostarczenia skierowania). Jeśli „tak” zostaje wydrukowany bilet, z którym udaje się do strefy oczekiwania oczekując na wezwanie do gabinetu. Jeśli „nie” zostaje wydrukowany bilet do Rejestracji, gdzie może wyjaśnić sytuację (np. brak dokumentacji – skierowanie, brak EWUŚ).

W przypadku poradni i elektrodiagnostyki system kolejkowy należy zintegrować z Systemem Kontroli Dostępu. Wydrukowane bilety powinny zawierać unikalny dla każdego pacjenta kod kreskowy, który po przyłożeniu do dedykowanych do tego celu czytników powinien otworzyć dane przejście SKD. Szczegóły integracji należy ustalić na etapie realizacji z dostawcą systemu KD.

Wezwanie pacjenta do danego stanowiska wywoływane jest ręcznie przez pracownika – realizowane jest to przez dedykowane oprogramowanie instalowane na stanowiskach komputerowych. Po wezwaniu na wyświetlaczu pojawia się wzywany numer wraz z graficzną informacją o wezwaniu. Wzywany numer pozostaje na wyświetlaczu do momentu wezwania nowego pacjenta lub zakończenia obsługi. Wezwanie pacjenta jest realizowane w formie audio-wizualnej. Na monitorach wyświetlany jest wzywany numer oraz podawany jest głosowy komunikat lub sygnał dźwiękowy. Dodatkowo na grupowych ekranach informacyjnych wyświetlana jest zbiorcza informacja o kolejkach i oczekujących numerach. Ekrany informacyjne powinny również umożliwić wyświetlanie komunikatów przygotowanych przez szpital.

Oprogramowanie

System powinien zapewnić uporządkowanie kolejności obsługi pacjentów w placówce poprzez rejestrację i przydzielenie do odpowiedniej kolejki, kierowanie pacjenta do odpowiednich stanowisk z zachowaniem pobranego numeru kolejkowego. Wymagane jest, aby system był w pełni zintegrowany z oprogramowaniem medycznym szpitala HIS – uprzednio zarejestrowany na daną godzinę pacjent w automacie biletowym potwierdza swoją obecność i jest obsługiwany „poza kolejką".

Wymagane jest, aby dostarczone oprogramowanie posiadało licencje bezterminowe. Dodatkowo musi istnieć możliwość rozbudowy systemu kolejkowego w przyszłości o kolejne grupy usług wybierane z panelu dotykowego automatu biletowego, dodatkowe stanowiska obsługi przy założeniu jednej jednostki zarządzającej pracą systemu i jednego programu sterującego. Wykonawca zobowiązany jest dostarczyć kompletny system zgodnie z dokumentacją projektową, oprogramowanie serwerowe do zarządzania systemem, aplikacji do zarządzania wyświetlaczami LCD, aplikacji do zarządzania automatami biletowymi oraz aplikacji do obsługi systemu w punktach obsługi pacjenta w ilości adekwatnej do ilości monitorów.

Oprogramowanie powinno zawierać poniższe funkcjonalne moduły:

- moduł dla administratora systemu
  - → Uwierzytelnianie i autoryzacja dostępu do panelu
  - → Dostęp do modułu poprzez interfejs www - możliwość kontroli pracy osobom odpowiedzialnym za nadzór bez konieczności opuszczania swoich miejsc pracy i instalowania dodatkowego oprogramowania
  - → Interfejs systemu wyłącznie w języku polskim
  - → Zarządzanie użytkownikami systemu oraz ich uprawnieniami
  - → Zarządzanie urządzeniami (wyświetlacze LCD, bileter)
  - → Zarządzanie kolejkami (dodawanie, usuwanie, blokowanie; definiowanie czasu pracy)
  - → Zarządzanie stanowiskami (dodawanie, usuwanie, blokowanie)
  - → Zarządzanie harmonogramami pracy,
  - → Zarządzanie kompozycjami wyświetlaczy, biletów, automatów biletowych
  - → Zarządzanie powiązaniami wyświetlaczy stanowiskowych ze stanowiskami, kolejek z wyświetlaczami grupowymi (możliwość wyświetlania stanu tylko wybranych kolejek), kolejek z zapowiedziami głosowymi (możliwość wygłaszania zapowiedzi tylko z wybranych kolejek), kolejek z automatami biletowymi (możliwość rejestrowania tylko do wybranych kolejek), kolejek ze stanowiskami
  - → System musi umożliwiać przydzielenie wybranych kolejek lub ich grup do każdego z pracowników osobno
  - → System musi umożliwiać tworzenie nieograniczonej ilości kolejek i dowolnego ich grupowania
  - → Zarządzanie treścią wyświetlaną na poszczególnych wyświetlaczach i automatach biletowych
  - → Zarządzanie treścią drukowaną na biletach (np. numer klienta wraz z symbolem literowym danej kategorii, datę i godzinę wydania biletu, miejsce do którego jest kierowany posiadacz biletu – poradnia)
  - → Konfiguracja parametrów systemu
  - → Dla każdej kolejki możliwość zdefiniowania indywidualnego, jedno- lub kilku-znakowanego prefiksu z określoną ilością zer wiodących
  - → Możliwość zdefiniowania słownika dni wolnych od pracy
  - → System kolejkowy działa na serwerze i jest uruchamiany automatycznie podczas włączania serwera - system musi działać na serwerze bez konieczności jego ręcznego uruchamiania

- moduł rejestracji klienta (obsługa automatu biletowego)

- → Konfigurowana lista obsługiwanych kolejek (stanowisk/gabinetów)
- → Rejestracja klienta w wybranej kolejce
- → Przejrzysty interfejs
- → Możliwość zdefiniowania własnych kompozycji min. tło, nagłówek ekranu startowego, kolory czcionki, kolory przycisków i tekstów, wielkości przycisków, kolor komunikatów
- → Wydruk biletu kolejkowego zawierającego treść zdefiniowaną przez administratora np. dowolny tekst, numer pacjenta, znak graficzny, data i czas wydruku, przewidywany czas oczekiwania, liczba oczekujących, kod kreskowy lub QR Code, spis dokumentów do załatwienia sprawy
- → Rejestrowane statystyki wydanych biletów
- → Możliwość blokowania na żądanie wydawania biletów i rejestracji pacjentów z danego automatu
- → System zapewnia wydawanie biletów w godzinach pracy wskazanych przez Zamawiającego (z możliwością osobnej konfiguracji harmonogramu pracy dla każdego dnia tygodnia i dla każdej kolejki osobno)
- → W systemie powinna istnieć możliwość samodzielnego określenia ilościowego lub czasowego limitu wydawania biletów do poszczególnych grup usług
- → Wybieranie poszczególnych kolejek powinno być możliwe w trybie wieloekranowym (menu hierarchiczne) np. przycisk główny „rejestracja” › podmenu: „rejestracja do poradni okulistycznej”, „rejestracja do poradni chirurgicznej” itd.

- moduł obsługi klienta – operacje wykonywane przez obsługę stanowisk (obsługa rejestracji i gabinetów lekarskich)
  - → Aplikacja instalowana na komputerach stanowiskowych posiadanych przez Zamawiającego
  - → Uwierzytelnianie i autoryzacja dostępu - logowanie użytkowników poprzez wprowadzenie osobistego loginu i hasła umożliwiającego przypisanie danych statystycznych do pracownika lub poprzez Active Directory
  - → Przejrzysty interfejs
  - → Możliwość umieszczenia/ zadokowania okna programu terminala stanowiskowego u góry lub z boku ekranu (w postaci np. paska narzędziowego) bez zasłaniania okna aplikacji systemu medycznego – zapewniające operatorowi możliwość ciągłej i jednoczesnej pracy z obydwoma programami bez konieczności ciągłego przełączania się pomiędzy oknem systemu medycznego a oknem terminala stanowiskowego systemu kolejkowego lub korzystania z dodatkowego monitora
  - → Prezentacja ilości osób oczekujących (oraz osób odłożonych w trybie widoku rozszerzonego)
  - → Przywołanie pacjenta do gabinetu wg kolejności wynikającej z kolejki
  - → Przywołanie pacjenta poza kolejnością (w trybie widoku rozszerzonego)
  - → Wezwanie, rozpoczęcie i zakończenie obsługi realizowane 1 przyciskiem w trybie widoku standardowego – pasek narzędziowy
  - → Usunięcie pacjenta z kolejki, gdy nie zgłosił się do obsługi mimo kilku wezwań (ręcznie w trybie rozszerzonym lub automatycznie po konfigurowalnej ilości wezwań)
  - → Aplikacja musi służyć do wstrzymania obsługi dowolnego pacjenta i odesłanie go na koniec, początek lub zawieszenia jego obsługi do wezwania
  - → Możliwość ponownego przywołania zawieszonego pacjenta
  - → Dowolny transfer między kolejkami bez konieczności ponownego pobierania biletu przez pacjenta z możliwością wskazania miejsca w kolejce, do którego ma trafić (na początek, na koniec, za określonym numerem)
  - → Możliwość przełączania się pomiędzy usługami (np. w przypadku nieobecności pracownika obsługującego inną kolejkę)
  - → każde stanowisko może obsługiwać więcej niż jedna kolejkę

→ Możliwość ręcznej rejestracji pacjenta do kolejki/poradni nawet mimo braku wpisu w terminarzu z możliwością zwiększenia priorytetu np. dla kombatantów, dawców krwi, osób niepełnosprawnych itp.
→ Możliwość wywołania podglądu (w trybie okna rozszerzonego) statystyki (ilości) klientów oczekujących w kolejce z podziałem na pilni, stabilni, zawieszeni, z przeniesienia
→ Możliwość wezwania pacjenta z każdej z pozostałych, nieobsługiwanych standardowo na danym stanowisku kolejek
→ Możliwość wyłączenia stanowiska pracy
→ Możliwość automatycznej aktualizacji aplikacji z serwera systemu kolejkowego

- moduł prezentacji informacji – wyświetlacze LCD
  → Wyświetlanie informacji o aktualnym stanie kolejek do stanowisk
  → Konfigurowany układ informacji – możliwość wyświetlania dodatkowych informacji multimedialnych jak pokaz slajdów, odtwarzanie filmów, paski tekstowe w oddzielnej strefie ekranu lub naprzemiennie z ekranem wyświetlacza grupowego
  → Konfigurowana ilość wyświetlanych najbliższych numerów
  → Możliwość zdefiniowania i zarządzania własnymi kompozycjami wyświetlaczy (kolory czcionek, kolor tła, marginesy, obramowania)
  → Wyświetlanie informacji tylko z tych kolejek, w których są osoby oczekujące
  → W przypadku większej ilości kolejek, automatyczne przełączanie na strony
  → Zdalny monitoring pracy wyświetlaczy w postaci aktualnego zrzutu ekranu, obciążenia procesora, zajętości pamięci RAM i dysku twardego, adresu IP, adresu MAC, uptime'u, aktualnego czasu na urządzeniu
  → Możliwość zdefiniowania tygodniowego harmonogramu pracy urządzeń (automatycznego włączania [przez WakeOnLan] i wyłączania o określonej godzinie w określone dni)

- moduł zapowiedzi głosowe
  → Nagłośnienie realizowane za pomocą głośników wbudowanych w wyświetlacze grupowe LCD
  → Dla każdej instancji zapowiedzi możliwość skonfigurowania indywidualnej listy obsługiwanych kolejek
  → System generuje i odtwarza zapowiedzi słowne informujące o zaproszeniu klienta do stanowiska. Zapowiedź może zawierać numer biletu, numer stanowiska, numer pokoju, numer gabinetu lub numer piętra
  → Możliwość ustawienia pełnej zapowiedzi lub gong

- moduł statystyk
  → Uwierzytelnianie i autoryzacja dostępu do panelu
  → Dostęp do modułu poprzez interfejs www - możliwość kontroli pracy osobom odpowiedzialnym za nadzór bez konieczności opuszczania swoich miejsc pracy i instalowania dodatkowego oprogramowania
  → Interfejs systemu wyłącznie w języku polskim
  → Możliwość zbierania i przetwarzania danych statystycznych o pracy systemu
  → Podgląd bieżącego statusu pracy stanowisk (stan, ostatnio wzywany numer, ilość obsłużonych klientów, średni czas oczekiwania, średni czas obsługi), kolejek (ilość oczekujących, ilość obsłużonych, średni czas oczekiwania, średni czas obsługi)
  → Obliczanie efektywności pracy elementów systemu w wybranym czasie i w rozbiciu na godziny dla: stanowisk (średnia ilość obsługiwanych klientów, średni czas obsługi, średni czas oczekiwania), kolejek (średnia ilość obsługiwanych klientów, średni czas obsługi, średni czas oczekiwania), operatorów (średnia ilość obsługiwanych klientów,

średni czas obsługi, średni czas oczekiwania), automatów biletowych (średnia ilość drukowanych biletów)
- → Obliczanie sumarycznych wartości monitorowanych wskaźników w wybranym czasie i w rozbiciu na godziny dla: stanowisk (ilość obsługiwanych klientów, czas obsługi, czas oczekiwania), kolejek (ilość obsługiwanych klientów, czas obsługi, czas oczekiwania), operatorów (ilość obsługiwanych klientów, czas obsługi, czas oczekiwania), automatów biletowych (ilość drukowanych biletów)
- → Możliwość przeglądania danych niezagregowanych (osobno dla każdego dnia z wybranego przedziału)
- → Moduł raportów e-mailowych z możliwością zdefiniowania nieograniczonej ilości raportów dobowych, tygodniowych, miesięcznych i rocznych, badających efektywność stanowisk, kolejek i operatorów w zakresie: całkowity czas pracy; liczba obsłużonych klientów; liczba osób, które zrezygnowały z obsługi; liczba osób, które czekały krócej niż 5 minut; maksymalny czas obsługi; maksymalny czas oczekiwania; procent obsłużonych klientów; procent klientów, którzy zrezygnowali z obsługi; procent osób, które czekały krócej niż 5 minut; średni czas obsługi; średni czas oczekiwania
- → możliwość wydruków raportów z systemu oraz możliwość eksportowania raportów i analiz do formatu pdf i csv, do samodzielnego wykonania przez Zamawiającego
- → Dostęp do logów z pracy systemu
- → Statystyki muszą pozwolić na obliczenie poniższych wskaźników:
  - ilość wydawania numerów w określonym przedziale dni w podziale na godziny,
  - wydajność pracy poszczególnych pracowników (liczba obsłużonych klientów),
  - czasy oczekiwania na obsługę,
  - czasy obsługi klientów

Integracja z systemem medycznym

Dostarczany system kolejkowy musi być zintegrowany z posiadanym przez Zamawiającego systemem medycznym w celu kolejkowania, kierowania i przywołania pacjentów. System kolejkowy musi zostać zintegrowany z systemem medycznym tak, aby możliwe było:

- → potwierdzenie przyjścia pacjenta w dniu planowanej wizyty oraz wyświetlenie informacji zwrotnej dla pacjenta generowanej przez system HIS (poradnia, godzina, lekarz)
- → skierowanie pacjenta do Rejestracji w przypadku braku potwierdzonego statusu EWUŚ (musi istnieć możliwość zdefiniowania, która kolejka do rejestracji obsługuje daną poradnię np. pacjent zostanie skierowany do kolejki „Rejestracja do poradni chirurgicznej" jeśli miał termin do „Poradni chirurgicznej", ale nie ma potwierdzonego statusu EWUŚ)
- → wymuszenie przez personel Rejestracji skierowania pacjenta do Rejestracji nawet mimo potwierdzonego statusu EWUŚ np. w celu uzupełnienia skierowania
- → na stanowisku Rejestracji możliwość wydruku biletu do poradni mimo braku potwierdzonego statusu EWUŚ (np. po podpisaniu oświadczenia przez pacjenta)

Dla pacjentów będących w poradni, w celu umówienia się na wizytę

Pacjenci maja możliwość zarejestrowania się do gabinetów lekarskich w ramach poradni. W tym celu po przyjściu do poradni pacjent powinien wybrać na ekranie dotykowym automatu biletowego odpowiedni przycisk pobrać bilet kolejkowy. W pierwszej kolejności Pacjent trafia do Rejestracji, gdzie obsługa rejestruje Pacjenta na dogodny termin, korzystając do tego celu z terminarzy systemu medycznego.

Jeśli istnieje możliwość, aby Pacjent został przyjęty przez lekarza w dniu rejestracji obsługa powinna wydać mu numer kolejkowy (wydruk za pomocą stacjonarnej drukarki termicznej), kierujący Pacjenta do odpowiedniego gabinetu.

Dla pacjentów już umówionych na wizytę lekarską

Pacjent po przyjściu do poradni powinien wybrać na ekranie dotykowym automatu biletowego odpowiedni przycisk i potwierdzić swoje przybycie poprzez wpisanie swojego numeru PESEL. Tym samym system kolejkowy wysyła zapytanie do terminarza systemu, aby potwierdzić, że dana osoba jest umówiona.

- → Jeśli wizyta zostanie potwierdzona pacjent otrzyma bilet kolejkowy kierujący go do odpowiedniego gabinetu lekarskiego, gdzie lekarz przywołuje Pacjenta do gabinetu za pomocą aplikacji systemu kolejkowego. Lekarz za pomocą terminarzy w systemie może umówić Pacjenta na kolejną wizytę.
- → Jeśli okaże się, że w terminarzu nie widnieje pozycja rejestracji na ekranie automatu biletowego powinien pojawić się komunikat o błędzie i skierowaniu Pacjenta do rejestracji w celu wyjaśnienia.

Pozostałe wymagania integracji

- → priorytetowym systemem musi być system medyczny, z którego system kolejkowy ma pobierać informacje z terminarza.
- → system kolejkowy nie może dokonywać żadnych wpisów do terminarzy (dostęp wyłącznie tylko-do-odczytu).

Integracja z Systemem Kontroli Dostępu

W celu integracji Systemu Kolejkowego z Systemem Kontroli Dostępu muszą zostać spełnione następującego założenia:

- → w trybie offline tzn. bez połączenia miedzy systemem Systemem Kolejkowym i SKD,
- → dla każdej kolejki zostaną zdefiniowane kody 2D/QR drukowane na biletach (w porozumieniu z dostawcą SKD),
- → czytniki SKD musza mieć zaprogramowana listę kodów, które będą umożliwiały przejście,
- → wartości kodów będą stale w czasie i dla każdego pacjenta.

Okablowanie

System do komunikacji będzie korzystał z projektowanego okablowania sieci strukturalnej. Lokalizacja gniazd LAN na rysunkach sieci strukturalnej.

Zasilanie urządzeń systemu wg branży elektrycznej.

Inne wymagania

Wykonawca zobowiązany do dostarczenia, zainstalowania oraz skonfigurowania oprogramowania systemowego i oprogramowania zarządzająco-sterującego dla wszystkich wskazanych w projekcie urządzeń. Dodatkowo zobowiązany do przeprowadzenia szkolenia w zakresie obsługi urządzeń i zainstalowanego oprogramowania dla administratorów. Wymagane jest także dostarczenie instrukcji obsługi w języku polskim dotyczącej eksploatacji poszczególnych urządzeń systemu i postępowania w przypadku awarii oraz instrukcji w języku polskim dotyczącej konfiguracji oprogramowania.

W pobliżu automatów biletowych wykonawca umieści tablicę informacyjną opisującą zasady działania systemu kolejkowego. Tablica powinna być wykonana, np. na plexi o formacie min. A3. Projekt tablicy musi zostać zaakceptowany przez Zamawiającego na etapie realizacji.

System powinien być objęty min. 2 letnią gwarancją. W okresie gwarancyjnym należy zapewnić max. 4-godzinny czas reakcji od zgłoszenia usterki/awarii, a naprawa powinna zostać wykonana w ciągu max. 24 godzin od zgłoszenia awarii poprzez serwis producenta. W ramach wsparcia Wykonawca zapewni kwartalną aktualizację oprogramowania (o ile zostanie wydane przez

Producenta) oraz zapewni wsparcie zdalne dla oprogramowania systemu kolejkowego za pomocą sieci Internet.

Wykonawca systemu oraz firma serwisująca musi posiadać stosowne certyfikaty oraz autoryzację Producenta. Wykonawca musi dołączyć do oferty deklarację zgodności dla sprzętu z normą bezpieczeństwa CE. Do oferty należy dołączyć karty katalogowe proponowanych urządzeń, wizualizacje graficzne oraz rysunki techniczne z wymiarami.

Wymagane jest, aby Wykonawca posiadał wdrożony Zintegrowany System Serwisowy, który w sprawny sposób umożliwia zgłoszenia awarii urządzeń oraz śledzenie statusów napraw. Wymagane jest, aby zgłoszenie problemów technicznych było dokonywane drogą elektroniczną przez osobę odpowiedzialną i upoważnioną po stronie Zamawiającego, mającą dostęp do portalu poprzez login i hasło. Oferent udostępni link do tego serwisu oraz testowy login oraz testowe hasło dostępu wraz ze złożeniem oferty. Do oferty należy dołączyć link, login oraz hasło do testowego użytkownika systemu. Internetowy system przyjmowania sprzętu do serwisu powinien zapewniać:

- → uzyskanie danych o dostarczonych produktach w szczególności o terminie ważności gwarancji
- → uzyskanie informacji o elementach składowych produktu, jeżeli jest wytworzony przez oferenta
- → podgląd dokonanych w trakcie eksploatacji wymian podzespołów
- → podgląd dołączonych do produktu dokumentów, w szczególności certyfikatów, zaświadczeń
- → uzyskanie historii awarii produktu oraz podjętych interwencji
- → powiadamianie Zamawiającego drogą elektroniczną (np. e-mail) o podjętych czynnościach w ramach zarejestrowanego zgłoszenia (np. określenie terminu usunięcia usterki, określenie terminu planowanej wizyty serwisowej wraz z opisem planowanych czynności, zamknięcie zgłoszenia serwisowego)
- → możliwość zgłaszania propozycji dotyczących funkcjonalności oprogramowania
- → możliwość zgłaszania błędów w oprogramowaniu
- → zarejestrowanie zgłoszenia reklamacyjnego
- → śledzenie stanu obsługi zgłoszenia reklamacyjnego od momentu zarejestrowania do jego zamknięcia

Minimalne parametry urządzeń

Wyświetlacz grupowy

Obudowa: fabryczna, wiszaca z przeznaczeniem do użytkowania wewnątrz budynków, matryca zabezpieczona szybą, montaż za pomocą dedykowanego uchwytu ściennego lub sufitowego

Monitor:

- Wielkość ekranu min 42”
- Rodzaj wyświetlacza: technologia S-IPS z krawędziowym podświetleniem LED
- Kontrast 1300:1
- Jasność (przy wysyłce) [cd/m²] 450
- Kąty widzenia [°] 178 poziomo / 178 pionowo
- Częstotliwość odświeżania obrazu [Hz] 60
- Rozdzielczość min. 1920 x 1080 przy 60 Hz

Terminal sterujący:

- Obudowa Mini PC
- Procesor dwurdzeniowy

- Pamięć RAM 2 GB
- Dysk SSD 64 GB
- Grafika HD
- Komunikacja LAN 10/100/1000
- WiFi 802.11 a/b/g/n/ac
- Porty w tylnej części 1 x VGA (15 pin D-Sub), 1 x HDMI, 6 x USB

Zasilanie 230V, 50Hz, pobór mocy. 150W

Automat biletowy

Obudowa:

- wolnostojąca z przeznaczeniem do użytkowania wewnątrz budynków odporna na akty wandalizmu, uniemożliwiająca dostęp z zewnątrz do podzespołów wewnętrznych i jakichkolwiek połączeń
- konstrukcja zewnętrzna wykonana z blachy stalowej o konstrukcji samonośnej zapewniającej sztywność i stabilność obudowy
- podstawa umożliwiająca trwałe zamocowanie do podłoża
- na froncie obudowy możliwość umieszczenia loga lub grafiki zgodnie z wymaganiami Zamawiającego
- kolorystyka dowolna, zgodnie z ustaleniami z Zamawiającym

Monitor:

- Przekątna monitora 19”
- Rodzaj wyświetlacza IPS TFT
- Czas reakcji matrycy 6 ms
- Kąty widzenia obrazu 178o poziomo / 178o pionowo (CR 10:1)
- Jasność [cd/m2] 250
- Kontrast 1000:1
- Rozdzielczość 1280 x 1024 @ 60Hz

Nakładka dotykowa:

- Przekątna 19”
- Technologia detekcji dotyku pojemnościowa
- Twardość powierzchni 7H w skali Mohsa
- Przejrzystość 90%

Komputer:

- Procesor 2.8 GHz
- Pamięć 2 GB
- Dysk twardy 64 GB SSD
- Interfejs graficzny zintegrowany
- Interfejs sieciowy zintegrowany, 10/100/1000 MBit/s
- Interfejs dźwiękowy zintegrowany
- Porty I/O 4x USB 2.0

Zasilanie: 230V, 50Hz, pobór mocy max. 350W

Drukarka biletów

- Metoda druku termiczna
- Prędkość wydruku 200 mm/s
- Szerokość papieru 50 - 90 mm
- Obcinacz cięcie pełne/częściowe
- Polskie znaki w wydrukach tekstowych CP852, Windows 1250
- Interfejs komunikacyjny USB + dodatkowy port

Serwer

- Procesor: 3.30 GHz (8MB cache)
- Liczba procesorów: 1
- Rodzaj pamięci: DDR3 Unbuffered ECC, 1600 Mhz
- Pojemność pamięci 8 GB
- Ilość slotów pamięci: 4
- Kontroler dysków SAS 2.0 (6Gbit) 0,1,10,5,50,6,60 512 MB
- Dyski 300 GB SAS, SFF, hot swap
- Zintegrowana karta sieciowa: 2 x Gigabit Ethernet, 10/100/1000 Mbps
- Napęd DVD RW
- Porty I/O: 2x RJ-45 (porty Gigabit Ethernet)
- 4 x USB 2.0:
- 1 x Video 15-pin (DB15),
- Zasilacz 2 x 450W, hot-plug
- Obudowa serwerowa Rack 1U

4.1.16 Szpitalny system informatyczny

W projekcie przewidziano miejsce w szafach RACK w serwerowni na przenoszone i rozbudowywane przez Inwestora serwery systemu HIS. Przenoszona będzie baza danych systemu informatycznego z obiektu przy ul. Krysiewicza. Prace związane z przenoszeniem należy uzgodnić z Inwestorem.

4.1.17 Integracja sal operacyjnych i endoskopowych

Założenia ogólne

Projektuje się wyposażenie obiektu w system integracji sal operacyjnych i endoskopowych.

System pozwoli na zintegrowanie wyposażenia medycznego jak i systemów technicznych wraz z systemami informatycznymi HIS/PACS/RIS. Elementy interfejsu (np. panele operatorskie) zapewniają kompleksowe sterowanie innymi systemami, system umożliwiać będzie integrację i sterowanie systemami technicznymi (np. urządzeniami wentylacyjnymi, oświetleniem ogólnym) i medycznymi (m. in. sterowanie funkcjami stołów i lamp operacyjnych). Możliwe będzie zarządzanie sygnałem wideo z urządzeń medycznych i kamer. Zarządzanie obrazem w obrębie sali umożliwia wyświetlenie dowolnego podłączonego źródła na wybrany monitor. Technologia zarządzania obrazem pozwoli na wykorzystanie go dla celów edukacyjnych, prezentacyjnych i archiwizowania danych. Materiał uzyskiwany z systemu integracji może być wykorzystywany do celów dydaktycznych poprzez prezentowanie wysokiej jakości wideo wraz z transmisją audio, umożliwiającą powstanie i funkcjonowanie systemu edukacyjnego. Transmisja obrazu i audio odbywa się może przy wykorzystaniu sieci Ethernet. System integruje się ze szpitalnym systemem informatycznym (HIS), a aplikacje odpowiedzialne z akwizycję i przesyłanie medycznych obrazów diagnostycznych są zgodne ze standardem DICOM.

Modułowość systemu pozwala na elastyczne dopasowanie funkcjonalności do wymagań personelu pracującego na sali operacyjnej oraz łatwą rozbudowę o dodatkowe moduły w przyszłości.

Funkcjonalności poszczególnych elementów systemu

[A.3]	**Sieciowa licencja stanowiskowa systemu dokumentacji badań endoskopowych**
Licencja zainstalowana na komputerze **[A.5]**	

System dokumentacji obsługuje wszystkie czynności wykonywane w nowoczesnej pracowni endoskopowej.

Funkcje:

- Interfejs programu w języku polskim,
- Oprogramowanie oparte na profesjonalnej, komercyjnej bazie danych SQL Server,
- Terminarz do prowadzenia zapisów badań, listy roboczej
- Zarządzenie prawami dostępu do programu i funkcji dla każdego użytkownika z możliwością autoryzacji poprzez indywidualne karty RFID
- Elektroniczna historia pacjenta z zapisem wyników badań, zdjęć, filmów bezpośrednio na nośnik CD/DVD
- Wyszukiwanie pacjentów po danych: PESEL, nazwisko, imię, data ur., nr księgi głównej
- Sterowanie rejestracją zdjęć i sekwencji wideo w jakości FullHD bezpośrednio z przycisków na głowicy kompatybilnego endoskopu lub przycisku nożnego
- Automatyczny transfer danych pacjenta (PESEL, nazwisko, imię, data ur.) na monitor zestawu endoskopowego
- Eksport opisów badań w formatach PDF i TXT
- Tworzenie dowolnych zestawień statystycznych, np. liczba wykonanych badań, ilość schorzeń, instytucje kierujące przy użyciu kreatora zapytań lub przez polecenia SQL,
- Eksport oraz import plików w formatach: BMP, JPG, PNG, PDF, TXT, AVI, MPG2 na nośnik typu pendrive/USB Flash
- Edycja obrazów przez nanoszenie warstwy z adnotacjami w postaci linii, strzałek, figur geometrycznych, tekstu, pomiarów planimetrycznych oraz edytor sekwencji wideo,
- Identyfikacja podłączonego endoskopu z podaniem typu i numeru seryjnego dla kompatybilnych urządzeń,
- Funkcja nagrywania notatek głosowych do badania,
- Zaznaczanie na schemacie anatomicznym miejsca rejestracji zdjęcia, pobrania wycinków oraz możliwość bezpośredniego drukowania skierowania do laboratorium,

- Tworzenie raportów z badań w oparciu o bloki tekstowe z możliwością zapisu własnych opisów badań do późniejszego wykorzystania i edycji raportu,
- Szablon opisu badania ze zdjęciami zarejestrowanymi podczas badania
- Tworzenie raportów z badań w oparciu o terminologię MST w języku polskim dla dolnego i górnego odcinka pokarmowego oraz dróg żółciowych, i dróg oddechowych
- Możliwość rozbudowy systemu o kolejne stanowiska robocze w architekturze klient-serwer,
- Moduł integracji procesu dezynfekcji w myjniach i przechowywania endoskopów w szafie endoskopowej
- System kompatybilny i przygotowany do integracji z systemami szpitalnymi typu HIS/RIS/PACS przez protokoły HL7 i DICOM oraz DICOM Worklist
- Autoryzowane szkolenie dla co najmniej 8 użytkowników systemu potwierdzone certyfikatem uczestnictwa

[A.5]	**Zestaw komputerowy dedykowany do systemu dokumentacji badań endoskopowych**
Biurko w pracowni endoskopowej z dostępem do sieci LAN	

Komputerowe stanowisko robocze systemu dokumentacji badań endoskopowych składa się z:

Stacja robocza:

• Płyta główna	oparta na chipsecie Intel
• Porty zewnętrzne	co najmniej 2 x COM RS232 złącze DB9
• Procesor	Intel Core i5
• Pamięć RAM	nie mniej niż 8 GB
• Przestrzeń dyskowa	SSD nie mniej niż 500 GB
• Karta graficzna	Intel HD,
• Napęd optyczny	nagrywarka DVD+/-RW z tacką
• Karta dźwiękowa	zintegrowana, zgodna z HD Audio
• Mikrofon	tak
• Karta sieciowa	zintegrowana na płycie 10/100/1000 Mbit/s
• Obudowa	mini-tower w kolorze ustalonym

	przez zamawiającego dopasowanym do kolorystyki pracowni endoskopowej
• System operacyjny	Microsoft Windows 7 Professional PL 64-bit
• Mysz	USB optyczna bezprzewodowa z rolką
• Klawiatura	bezprzewodowa US/European (QWERTY)

Monitor LCD:

• Rozdzielczość	nie mniej niż 1920x1080 px
• Przekątna/proporcje ekranu:	nie mniej niż 21,5-cala / 16:9
• Wejścia	co najmniej 1 x DVI-D, 1 x D-SUB,
• Głośniki	2x2W

Laserowa drukarka kolorowa

• Prędkość druku (A4)	Do 18 stron na minutę (mono i kolor)
• Kolor obudowy	uzgodniony z zamawiającym nawiązujący do kolorystyki pracowni endoskopowej
• Interfejs lokalny	Hi-Speed USB 2.0
• Interfejs sieci	IEEE 802.11b/g/n

Zasilacz awaryjny UPS

• Moc pozorna/skuteczna	550 VA / 330 W
• Gniazda wyjściowe	230V PL –co najmniej 8szt.

Karta przechwytująca obraz w jakości FullHD kompatybilna z systemem dokumentacji badań endoskopowych [A.4]

• Interfejs	PCIe x4
• Wejście wideo	HD-SDI (SMPTE 292M)
• Rozdzielczość	co najmniej 1920x1080

[A.8 i A.9]	**Matryca przełączania sygnałów wideo z modułem 8 wejść i 8 wyjść w standardzie 3G-SDI**

Szafka techniczna dla endoskopii, wymiar 2U	

Zewnętrzna matryca kompatybilna z kontrolerem urządzeń medycznych pozwala na podłączenie źródeł i odbiorników obrazu wideo w standardzie 3G-SDI. Dystrybucja sygnałów wideo na monitory bez opóźnień w obrębie sali operacyjnej, sterowanie przełączaniem sygnałów odbywa się z monitora dotykowego systemu integracji.

Obsługa sygnałów wideo w rozdzielczości do 1080p50 pochodzących z następujących źródeł:

- kamera endoskopowa
- kamera w lampie operacyjnej
- kamera zewnętrzna podglądowa (naścienna lub sufitowa)
- kamera mikroskopu
- fluoroskop
- USG
- system dokumentacji badań endoskopowych

Funkcje i wyposażenie:

- co najmniej 7 wejść w standardzie single-link SDI, HD-SDI, 3G-SDI; lub dual-link HD-SDI
- co najmniej 8 wyjść w standardzie single-link SDI, HD-SDI, 3G-SDI; lub dual-link HD-SDI
- Możliwość współpracy z modułem 16 wejść i 16 wyjść wideo 3G-SDI
- Przepustowość wejść/wyjść min 2.97 Gbps
- Standard złącz wejść/wyjść wideo: BNC
- Port komunikacyjny RS-232, RS-422, złącze DB-9
- Port komunikacyjny Ethernet 10/100Base-T, half/full duplex
- Zasilanie sieciowe 100-240 VAC, 50-60 Hz

[A.1/B.1]	**Kontroler urządzeń medycznych**
Instalacja na półce kolumny chirurgicznej, min. głębokość półki 550 mm	

Sterowanie urządzeniami medycznymi poprzez ekrany dotykowe i komendy głosowe oraz interfejsy komunikacyjne umożliwiające sterowanie z obszaru sterylnego i nie sterylnego

urządzeniami takimi jak: insuflator, diatermia, nóż harmoniczny, źródło światła, wideoprocesor kamery endoskopowej, kamera lampy operacyjnej, monitory operacyjne, stół operacyjny, lampy operacyjne, kamera sali operacyjnej, urządzenie do archiwizacji. Wizualizacja graficzna przycisków sterujących i wartości parametrów urządzeń medycznych na ekranie dotykowym umożliwiająca intuicyjne sterowanie i kontrolę stanu pracy. Wspólny interfejs sterowania urządzaniami medycznymi oraz sygnałami audio/wideo. Funkcja scenariuszy zabiegów pozwala na zaprogramowanie i przywołanie parametrów urządzeń medycznych indywidualnie dla każdej procedury i użytkownika osobno. Dowolność konfiguracji scenariuszy przez użytkownika zapewnia standaryzację procedur chirurgicznych, skraca czas i ułatwia obsługę urządzeń.

Funkcje:

- Urządzenie medyczne klasy I wg dyrektywy medycznej 93/42/EEC
- Wspólny interfejs użytkownika z kontrolerem sygnałów audio-video,
- Sterowanie parametrami urządzeń systemu zintegrowanej sali operacyjnej z monitora dotykowego lub komendami głosowymi min.:
    - kamerą endoskopową FullHD i laparoskopową FullHD/3D/4K wraz ze źródłem światła w zakresie funkcji min. balans bieli, wł/wył lampy, jasność, przesłona, wzmocnienie, zoom, wyzwalacz, tryb 2D/3D (min. trzema urządzeniami równocześnie) ,
    - insuflatorem, w zakresie min. start/stop, ciśnienie, przepływ,
    - nożem harmonicznym albo zaawansowanym urządzeniem do koagulacji bipolarnej wysokiej energii
    - urządzenie do archiwizacji - rejestrator cyfrowy FullHD i 4K, w zakresie funkcji min. start/stop/pauza nagrywania, odtwórz, stop, pauza, zapis zdjęcia, dane pacjenta
    - lampami chirurgicznym w zakresie funkcji min. włącz/wyłącz, tryb endo, jasność, oraz kamerą w lampie w zakresie funkcji freeze, focus, zoom, obrót, przesłona, balans bieli, tryb 2D/3D
    - diatermią chirurgiczną (min. dwoma urządzeniami równocześnie),
    - stołem operacyjnym bezprzewodowo poprzez interfejs podczerwieni IR lub przewodowo z wykorzystaniem protokołu RS-232,
    - monitorem medycznym HD/3D/UltraHD/4K w zakresie funkcji min. wybór wejścia wideo, konfiguracja złożonych obrazów Picture in Picture / Picture by Picture, tryb 2D/3D (min. sześcioma monitorami równocześnie)

- oświetleniem sali w zakresie funkcji min. konfiguracji od 2 do 6 niezależnych stref, min. 4 zaprogramowane ustawienia, wyłączenie wszystkich stref
- kamerą obserwacyjną PTZ, w zakresie funkcji min. obracanie, pochylanie, zoom, focus, wywołanie jednego z sześciu zaprogramowanych położeń, (możliwość konfiguracji siedmiu kamer)
- urządzeniami niemedycznymi przez protokoły IR i RS232 oraz wyjścia przekaźnikowe **[A.10/B.16]**
- sterowanie zewnętrzną matrycą sygnałów wideo, z funkcją podglądu źródła obrazu na monitorze sterującym,
- możliwość podłączenia co najmniej dwóch dotykowych ekranów sterujących z funkcją indywidualnego dostosowania funkcji sterujących dla każdego osobno
- obsługa do 2 przycisków bezpieczeństwa dla stołu operacyjnego,
- możliwość sterowania oświetleniem sali, obsługa nie mniej niż 6 stref lub kolorów
- wejście mikrofonu dla funkcji sterowania głosowego,
- wyjście głośnikowe dla powiadomień i komunikatów głosowych,
- tworzenie co najmniej 40 zaprogramowanych profili użytkowników,
- dostęp użytkownika zabezpieczony hasłem,
- tworzenie ustawień automatycznych i scenariuszy zabiegów,
- przypisanie ustawień automatycznych i scenariuszy do użytkownika,
- odtwarzanie i zapis obrazów z/do pamięci USB,
- nadrzędność sterowania urządzeniami medycznymi bezpośrednio z ich paneli czołowych w stosunku do sterowania za pomocą interfejsu użytkownika

Kontroler urządzeń medycznych zapewnia kompatybilność w zakresie sterowania z: - min. trzema producentami stołów operacyjnych

- min. pięcioma producentami lamp i kamer operacyjnych
- min. trzema producentami urządzeń elektrochirurgicznych w zakresie sterowania
- min. dwoma producentami urządzeń do archiwizacji w jakości HD, 3D i 4K.

[B.6]	**Kontroler sygnałów audio-wideo**
Instalacja na półce kolumny chirurgicznej, min. głębokość półki 550 mm	

System umożliwia wyświetlenie i przekierowanie wybranego źródła obrazu wideo powstającego na sali operacyjnej na dowolnie wybrany odbiornik/wyjście wideo (monitory, ekran ścienny, rejestrator, wideokonferencja). Wspólny interfejs sterowania, monitor dotykowy z kontrolerem urządzeń medycznych, monitory mogą być zainstalowane na ramieniu mocowanym do sufitu lub wysięgniku montowanym do głowicy kolumny w strefie sterylnej sali operacyjnej - urządzenia posiadają certyfikat MDD lub w strefie niesterylnej na panelu ściennym. Dystrybucja sygnałów wideo na monitory odbywa się bez opóźnień w obrębie sali operacyjnej. Jednostka centralna wideoroutera zainstalowana na półce kolumny chirurgicznej w obrębie sali operacyjnej, miejsce instalacji umożliwia w przyszłości szybkie i łatwe podłączenie nowych urządzeń (źródeł wideo) bez konieczności prowadzenia dodatkowego okablowania. Graficzna wizualizacja na panelu sterującym skonfigurowanych ścieżek sygnałów wideo przekierowanych w obrębie sali i poza nią. Wbudowany mikser oraz wzmacniacz sygnałów audio pozwala na dowolną konfigurację sygnałów wejściowych i wyjściowych, takich jak: mikrofony bezprzewodowe dla operatora i asysty, połączenie konferencyjne, wejście zewnętrznego odtwarzacza audio (np. MP3), kanał audio zewnętrznego cyfrowego rejestratora medycznego oraz kanał audio zewnętrznego komputera. System jest wyposażony w parę pasywnych głośników sufitowych lub ściennych. Możliwość doposażenia systemu w zewnętrzny wzmacniacz audio o większej mocy. System wyposażony w zewnętrzną modułową matrycę sygnałów wideo z obsługa sygnałów w rozdzielczości HD/3D/UltraHD/4K zgodną ze standardami 3G/HD-SDI, DVI U (DVI, VGA, HDMI, RBGBHY, S-Video Y/C, Composite, YPbPR/YUV).

Funkcje:

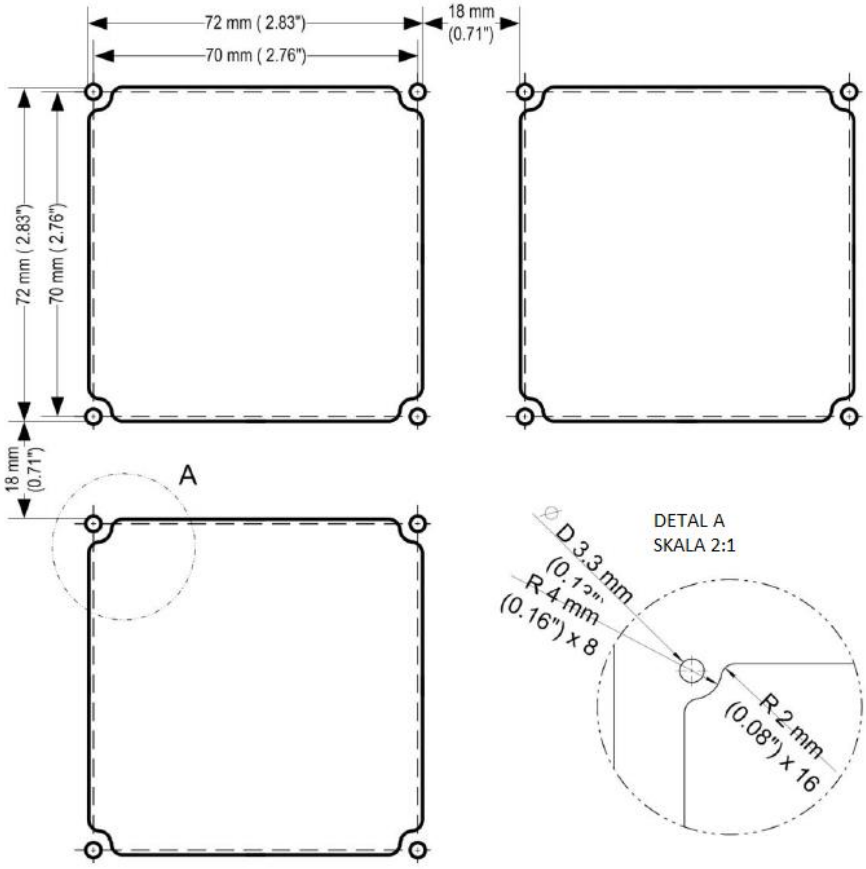
- Urządzenie medyczne klasy I wg dyrektywy medycznej 93/42/EEC
- Lampka On-Air sygnalizująca aktywną transmisję wideokonferencyjną, która może być zainstalowana wewnątrz lub na zewnątrz sali operacyjnej
- Funkcja telefonu IP poprzez protokół SIP oraz H.323 z wbudowaną książką adresową
- Intuicyjny interfejs użytkownika z podziałem na aplikacje
- Min. 2 porty USB na przednim panelu urządzenia
- współdzielenie interfejsu sterowania na ekranach dotykowych z kontrolerem urządzeń medycznych
- Podgląd aktualnie przełączanego źródła obrazu wideo na dotykowym ekranie sterującym, z funkcją full screen
- funkcja wydruku zapisanych zdjęć na drukarce sieciowej
- ochrona przed zmianami w konfiguracji systemu zabezpieczona hasłem
- użytkownik ma do dyspozycji co najmniej 40 zaprogramowanych nastaw/profili w systemie na jedną salę operacyjną

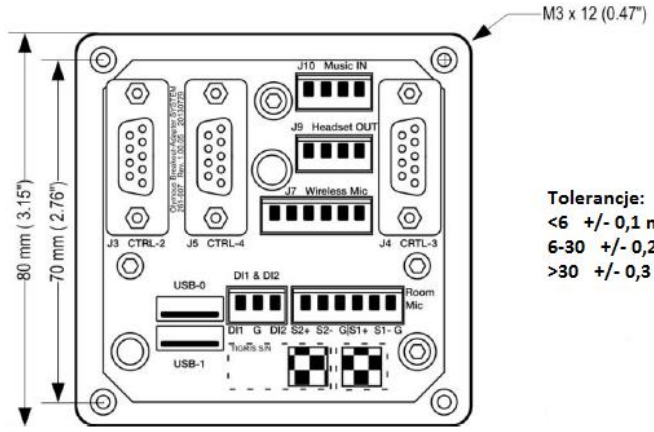
- Możliwość montaż routera AV w pomieszczeniu technicznym sąsiadującym z salą operacyjną dla serwisu i bioinżynierów
- możliwość sterowania co najmniej 2 kamer PTZ
- Możliwość integracji z systemem PACS przez protokół DICOM ze wsparciem dla usług: DICOM C-Store, DICOM Storage Commitment, DICOM Modality Worklist, DICOM Modality Performed Procedure Step,
- Możliwość rejestracja zdjęć i obrazu wideo,
- Możliwość automatycznego eksportu zarejestrowanych obrazów na USB, Share, VNA (Vendor Neutral Archive), PACS,
- Możliwość wdrożenia indywidualnej okołooperacyjnej listy kontrolnej z funkcją przekierowania na wszystkie lub wybrane monitory.
- Para głośników sufitowych lub ściennych **[B.22]**
- Wbudowany wzmacniacz i matryca sygnałów audio
- Możliwość sterowania kompatybilną matrycą w technologii Video Over IP w technologii światłowodowej
- System współpracuje z modułową matrycą sygnałów wideo **[B.17 i B.11]**
- Sterowanie sygnałami audio: głośniki, bezprzewodowy zestaw nagłowny, zewnętrzne źródło audio z wejściem mini jack 3,5mm lub bezprzewodowo przez Bluetooth wraz ze sterowaniem funkcjami odtwarzacza Start/Stop, Następy/Poprzedni utwór, tytuł, artysta, album z ekranu dotykowego systemu integracji. Zasięg Bluetooth do 10 metrów.
- Sterowanie zewnętrznymi komputerami (np. HIS/PACS/system do dokumentacji) przez ekran dotykowy min. do 4 komputerów.
- Mikrofon bezprzewodowy do komunikacji A/V przez sieć IP
- System kompatybilny z urządzeniami do wideokonferencji min. dwóch wiodących producentów. Funkcje dostępne z poziomu systemu:
    - książka adresowa lokalna i w kodeku,
    - sterowanie poziomem sygnałów audio,
    - wysłanie dowolnego obrazu z sali operacyjnej do lokalizacji zdalnej,
    - odbiór obrazu z lokalizacji zdalnej i przekierowanie na dowolne monitory,
    - podgląd obrazu wysyłanego i przychodzącego na ekranie dotykowym systemu integracji,
    - możliwość uczestniczenia w wideokonferencjach mostkowych (multi-point),
    - wykonywanie, odbieranie i odrzucanie połączeń z ekranu dotykowego systemu integracji,
    - do obsługi systemu wideokonferencji nie jest wymagany pilot zdalnego sterowania do urządzenia wideokonferencyjnego, wszystkie niezbędne funkcje dostępne z poziomu systemu intergacji.

- dedykowane moduły instalacyjne do kolumny chirurgicznej ograniczające ilość okablowania
- wbudowany enkoder do streamingu sygnału wideo i dwukierunkowego dźwięku do sieci LAN przez protokół TCP/IP
- możliwość streamingu 3 niezależnych sygnałów wideo
- wsparcie dla przełączania sygnałów HD, 3D, 4K i UltraHD.

[B.7]	**Zestaw przyłączy systemowych na kolumnę chirurgiczną (CSU) wraz z dedykowanym okablowaniem systemowym [B.8,9,10]**
Instalacja na bocznych ściankach kolumny chirurgicznej w otworach wg. rysunku.	

W związku z tym że kontroler urządzeń medycznych oraz sygnałów audio-wideo umiejscowione będą na kolumnie chirurgicznej, aby zminimalizować ilość okablowania zastosowano dedykowane gniazda instalacyjne, które pozwalają na ukrycie części okablowania wewnątrz kolumny chirurgicznej. Otwory będą wykonane przez producenta kolumn chirurgicznych.





Tolerancje:
<6 +/- 0,1 mm (0.004")
6-30 +/- 0,2 mm (0.008")>
>30 +/- 0,3 mm (0.01")

[A.6/B.12]	**Dotykowy monitor sterujący**
Instalacja na uchwycie naściennym z mocowaniem VESA 75/100	

Kolorowy ekran dotykowy o przekątnej min. 18". Aktywna matryca TFT LCD z podświetlaniem LED, służy do wyświetlanie interfejsu użytkownika systemu integracji sali operacyjnej. Możliwość podłączenie drugiego ekranu sterującego. Ekran w technologii dotykowej zainstalowany na regulowanym ramieniu do kolumny chirurgicznej lub na dedykowanym zawiesiu sufitowym lub ściennym.

Parametry:

- Urządzenie medyczne klasy I wg dyrektywy medycznej 93/42/EEC
- Rozdzielczości natywna 1920x1080 @ 50,60 Hz
- Technologia wyświetlacza: Active matrix TFT LCD (LED), 16,7 mln kolorów
- Kąt widzenia poziom/pion – min 178° / min 178°
- Przekątna ekranu: min.18 cali, proporcje 16:9
- Jasność: nie mniej niż 220 cd/m²
- Kontrast monitora: nie mniej niż 3000:1
- Interfejs HID: USB
- Technologia dotykowa: pojemnościowa 10 punktów
- Montaż: VESA 75, 100

[A.7/B.13]	**Kamera obserwacyjna PTZ**
Instalacja do sufitu na sali operacyjnej/endoskopowej	

System integracji umożliwia sterowanie kamerą PTZ, oraz przekierowanie obrazu wideo na dowolny odbiornik. Kamera kompatybilna z systemem integracji, zapewnia obraz w jakości Full HD. Szeroki zakres roboczy i płynne działanie funkcji PTZ (obrót/przechył/zbliżenie). Kamera wyposażona w funkcję odwracania obrazu, możliwość montażu na suficie. Sterowanie funkcjami kamery takimi jak obracanie, pochylanie i zbliżenie i wywołanie jednego z sześciu zaprogramowanych położeń oraz podgląd obrazu z kamery dostępne na dotykowym ekranie sterującym systemu integracji.

Parametry:

Rozdzielczość sygnału wideo 1080i

Typ sygnału wideo:	HD-SDI
Zakres obrotu:	min. 310°
Zakres pochylenia:	min. 90°
Prędkość max. obrotu/pochylenia:	40°/s
Powiększenie optyczne:	10x
Możliwość zapamiętania	min. 5 pozycji kamery
Możliwość montażu kamery	w pozycji standardowej lub odwróconej

[B.15]	**Dwustrefowy sterownik oświetlenia z modułem komunikacyjnym RS232 [B.14]**
Instalacja sterownika **[B.15]** na ścianie w sali operacyjnej, moduł komunikacyjny **[B.14]** w dedykowanej szafce technicznej	

Sterownik stanowi element wykonawczy i pozwala kontrolować oświetlenie sali operacyjnej w dwóch strefach lub kolorach. Za komunikację z systemem integracji odpowiedzialny jest moduł komunikacyjny **[B.14]**. który komunikuje się z modułem interfejsu kontrolera urządzeń medycznych. Należy zaprojektować oświetlenie sali tak aby sterownik w trybie ręcznym umożliwiał niezależne od systemu integracji sterowanie oświetleniem oraz poprzez tradycyjne włączniki ścienne.

[A.10/B.16]	**Kontroler urządzeń niemedycznych (3xRS232, 4xIR,4xRELAY)**
Instalacja na półce w dedykowanej szafce technicznej	

Kontroler kompatybilny z systemem integracji sali operacyjnej, pozwala sterować urządzeniami niemedycznymi takimi jak:- monitory, kamery sufitowe, oświetlenie, klimatyzacja, rolety. Wbudowane porty komunikacyjne RS232, podczerwień IR, wyjścia przekaźnikowe pozwalają na podłączenie różnych urządzeń. Komunikacja z systemem integracji odbywa się przez protokół TCP/IP. Dla konkretnego urządzenia, na podstawie dokumentacji i dostępnych komend, producent systemu integracji opracowuje indywidualnie sterownik w postaci pliku. Następnie sterownik wgrywany jest do systemu. Urządzenie może być sterowane z ekranu dotykowego systemu integracji.

[B.17]	**Modułowa matryca wideo kompatybilna z kontrolerem sygnałów audio-wideo wyposażona w moduły wejść wyjść**
Instalacja w dedykowanej szafce technicznej, poza sala operacyjną, montaż rack,	

wymiar 4RU

System integracji współpracuje z modułową matrycą sygnałów wideo, która pełni funkcję wykonawczą przełączania sygnałów wideo pomiędzy źródłami i odbiornikami na sali operacyjnej. Matryca wyposażona w sloty na 16 modułów wejść/wyjść, pozwala na zwiększenie ilości wejść i wyjść oraz obsługuje różne standardy wideo takie jak Composite, S-Video, RGBHV, VGA, YPbPR/YUV, 3G/HD-SDI, DVI/HDMI. Komunikacja pomiędzy matrycą a kontrolerem odbywa się przez protokół TCP/IP, sterowanie przełączaniem sygnałów odbywa się z poziomu ekranu dotykowego systemu integracji sali operacyjnej. Na ekranie sterującym wyświetlany jest podgląd obrazu. Matryca zapewnia konwersję pomiędzy standardami wideo i skalowanie sygnałów SD i HD, każde wejście SD lub HD może być przekierowane na dowolne wyjście SD lub HD, zapewnienie odwzorowania sygnału źródłowego w rozdzielczości natywnej monitora.

Okablowanie obejmuje wszystkie urządzenia źródłowe, wytwarzające obraz na sali operacyjnej, takie jak:

- kamera endoskopowa i laparoskopowa (w standardach HD/3D/4K)
- kamera w lampie operacyjnej HD/3D
- kamera zewnętrzna podglądowa PTZ (naścienna lub sufitowa)
- kamera mikroskopu
- fluoroskop
- USG
- komputer PACS/HIS, negatoskop cyfrowy, komputer instrumentariuszki
- stacja komputerowego wspomagania chirurgicznego (nawigacja chirurgiczna)

oraz wszystkie monitory/odbiorniki obrazu, takie jak:

- monitory operacyjne
- ścienny panel panoramiczny **[B.24]**
- system transmisji wideo po sieci TCP/IP **[C.6]**

Matryca zapewnia kompatybilność z sygnałami wideo o rozdzielczości HD/3D i 4K.

Funkcje i parametry:

Wejścia:

- min. 4 x HD-SDI **[B.19]**
- min. 8 x 3G-SDI **[B.20]**

Wyjścia:

- co najmniej 12 x 3G-SDI **[B.21]**

wsparcie dla :

- sygnałów 3G-SDI Level B (obrazowanie 3D)
- głębi kolorów BT.2020 (obrazowanie 4K).

[A.12/B.23]	**Mikrofon bezprzewodowy**
Instalacja w przestrzeni sufitowej na sali operacyjnej	

Mikrofon zapewnia komunikację głosową operatora podczas transmisji strumieniowych po sieci LAN. Zestaw wyposażony w miniaturowy nadajnik typu body-pack z mikrofonem krawatowym. Mikrofon zapewnia sprawną komunikację w występującym na Sali operacyjnej polu elektromagnetycznym oraz w trakcie wykonywania badań fluoroskopowych z wykorzystaniem promieniowania X.

[A.12/B.24]	**Naścienny ekran panoramiczny LCD**
Instalacja ścienna z mocowaniem w standardzie VESA na za panelem szklanym wykańczającym zabudowę ścian	

Urządzenie poprzez połączenie z matrycą wideo pozwala wyświetlić dowolny dostępny na sali obraz tym samym pełnić rolę negatoskopu cyfrowego, panelu konferencyjnego, monitora endoskopowego. Panel może służyć jako podgląd danych pacjenta z systemu HIS i dokumentacji obrazowej z systemu PACS po przekierowaniu sygnału z komputera dostępowego.

Parametry:

- Przekątna ekranu naściennego panelu: nie mniej niż 42”
- Rozdzielczość natywna: co najmniej 1920 x 1080 pikseli
- Proporcje ekranu: 16:9
- Wejścia sygnału video: 3G-SDI, DVI, HDMI.
- Interfejs RS-232 do komunikacji pomiędzy monitorem a systemem zintegrowanym sali operacyjnej.

[C.1]	**Serwer dedykowany do systemu systemu dokumentacji badań endoskopowych**
Szafa serwerowa rack IT, 1 RU	

Serwer utrzymuje bazę danych systemu dokumentacji i zarządzania badaniami w pracowni endoskopowej. Na serwerze uruchomione są usługi integracji z systemami szpitalnymi HIS i PACS oraz urządzeniami do rejestracji procesów dezynfekcji aparatów i przechowywania aparatów endoskopowych.

Parametry:

- Obudowa typu rack 1U
- Suwane szyny montażowe do szafy rack
- Procesor Intel Xeon E3
- Pamięć RAM min. 8GB (1x8GB)
- Zainstalowane dyski 4 x HD SATA min 6G 3TB 7.2K HOT PL 3.5" BC
- Napęd DVD-RW
- Kontroler (RAID 0, 1, 10, 5, 50)
- System operacyjny Windows Server 2012 R2 Standard
- Zasilacz nadmiarowy modułowy hot-swap PSU 450W platinum hp

[C.2]	**Licencja serwer bazy danych systemu dokumentacji badań endoskopowych**
Oprogramowanie zainstalowane na serwerze **[C.1]**	

Licencja podstawowa systemu dokumentacji utrzymuję bazę danych na silniku MS SQL oraz zapewnia funkcjonowanie systemu w architekturze serwer-klient w środowisku MS Windows

[C.3]	**Licencja systemu dokumentacji badań endoskopowych na moduł integracji systemem szpitalnym klasy HIS**
Oprogramowanie zainstalowane na serwerze **[C.1]**	

Licencja dodatkowa do systemu ENDOBASE zapewnia wsparcie dla standardu komunikacji pomiędzy systemami medycznymi typu HIS z wykorzystaniem protokołu HL7.

[C.4]	**Licencja systemu dokumentacji badań endoskopowych na moduł integracji systemem szpitalnym klasy PACS**
Oprogramowanie zainstalowane na serwerze **[C.1]**	

Licencja nie fizyczna do systemu zapewnia wsparcie dla standardu komunikacji pomiędzy systemami medycznymi typu PACS z wykorzystaniem protokołu DICOM.

[C.5]	**Licencja systemu dokumentacji badań endoskopowych na moduł integracji z automatycznymi myjniami-dezynfektorami i z szafami do przechowywania endoskopów w warunkach kontrolowanej atmosfery ochronnej**
Oprogramowanie zainstalowane na serwerze **[C.1]**	

Moduł integracji dla systemu dokumentacji badań endoskopowych uzupełnia przerwę w historii obsługi aparatu pomiędzy badaniami, zapewniając automatyczne, zdigitalizowane śledzenie aparatu co najmniej podczas:

- procesu dezynfekcji w myjniach automatycznych
- suszenia i przechowywania w szafach endoskopowych w warunkach kontrolnej atmosfery ochronnej
- użycia aparatu do badania

Oprogramowanie na bieżąco kontroluje status dezynfekcji aparatu przed użyciem do badania, w przypadku wykrycia nieprawidłowości, wyświetla ostrzeżenie dla operatora z informacją o przyczynie. Wbudowany w oprogramowanie moduł historii aparatu pozwala wyświetlić elektroniczny raport z każdego urządzenia biorącego udział w procesie mycia, dezynfekcji i przechowywania. Raport ten jest powiązany z rekordem badania i pacjenta i może być dołączony do wyniku badania dla pacjenta.

[C.6]	**Licencja systemu streamingu sygnałów audio-wideo**
Oprogramowanie zainstalowane na serwerze **[C.7]**	

Sieciowa platforma dystrybucji sygnałów audio-wideo pomiędzy salą operacyjną a zewnętrznymi odbiorcami (sala konferencyjna/seminaryjna/odpraw itp.). System umożliwia transmisję na żywo poprzez istniejącą lub dedykowaną sieć LAN, dowolnie wybranych sygnałów wideo wraz z dwustronną komunikacją głosową. Platforma wideo jest dostępna w całej sieci szpitalnej poprzez stronę www z dostępem dla autoryzowanych użytkowników lub przez konto gościa. Pełna konfiguracja poziomu uprawnień kont użytkowników z możliwością integracji z LDAP i Active Directory. Odbiór sygnału audio-wideo odbywa się za pomocą komputera klasy PC pracującego w lokalnej sieci LAN, przy użyciu odtwarzacza pobieranego automatycznie ze

strony platformy, odtwarzacz nie wymaga instalacji na komputerze. Opcjonalnie system umożliwia konfigurację widoku obrazów wideo z kilku źródeł niezależnie i wyświetlenie w indywidualnie konfigurowanym widoku (MultiView). System wykorzystuje transmisję Mulitcast oraz umożliwia konfigurację dwóch równoległych strumieni streamingu (High/Low) o różnym poziomie przepływności bitrate z jednego źródła wideo, umożliwia to wybór odbiorcy wybranej jakości obrazu, niższej np. dla urządzeń mobilnych. Enkodery wbudowane w kontroler audio-wideo współpracują z systemem integracji, włączenie lub wyłączenie sygnału wysyłanego do streamingu odbywa się z interfejsu ekranu dotykowego systemu inetgracji. O włączeniu transmisji decyduje wyłącznie operator na sali operacyjnej.

Funkcje systemu:

- Odbiór streamingu na dowolnym komputerze w sieci szpitalnej bez konieczności instalacji dodatkowego oprogramowania wraz z dwukierunkową komunikacją głosową
- Konfiguracja widoku MultiView w dowolnej konfiguracji wybranej przez użytkownika
- Niezależny odbiór obrazów z różnych źródeł wideo, streaming z kilku sal operacyjnych równocześnie
- Dowolna konfiguracja poziomu dostępu i uprawnień dla użytkowników i grup, możliwość ograniczenia funkcjonalności np. dostęp do kanału zwrotnego audio, wybranych transmisji z konkretnych sal operacyjnych
- Konto administratora systemu
- Wsparcie dla sieci Unicast i Multicast
- Funkcja integracji kont użytkowników systemu z LDAP i Active Directory
- Nieograniczona liczba odbiorców streamingu na żywo
- Transmisja obrazu FullHD 1080p, kodowanie h.264 szyfrowane AES 256
- System pracuje w istniejącej infrastrukturze sieciowej LAN 1Gbit

Parametry enkodera:

- Możliwość wbudowania do 3 enkoderów wewnątrz kontrolera sygnałów audio-wideo, daje możliwość wysłania 3 niezależnych transmisji wideo na żywo z jednej sali operacyjnej.
- Urządzenie pozwalające na komunikację dwukierunkową audio-video przez protokół IP pomiędzy salą operacyjną i dowolnym komputerem w szpitalu
- Pełna integracja kodeka z systemem zintegrowanym, zarządzanie kodekiem z poziomu systemu zintegrowanego. Nie wymaga specjalistycznego okablowania do realizacji połączeń konferencyjnych - wykorzystanie szpitalnej sieci LAN,
- Aktualizacja oprogramowania systemowego przez sieć IP
- Wejście RJ-45 obsługujące 10/100/1000 Base-T Ethernet Network
- Protokoły IPv4,DHCP, IGMPv3 dla MultiCast IP

- Parametry STREAMING: MPEG2 Transport Stream as per ITU-T Rec. H.222.0 / ISOIEC 13818-1, Direct RTP - H.264 over RTP (RFC 3984)
- Obsługa protokołów RTP/RTCP (RFC 3550), SAP (RFC 2974), SDP (RFC 2327), RTSP (RFC 2326), Quick Time Stream (RFC 3984 video encapsulation and RFC 3640 AAC-LC audio payload)
- INTERFEJSY ZARZĄDZAJĄCE: HTTP (Web Browser), Command line TELNET, SSH lub RS-232 serial line, FTP/TFTP Client/Server, SNMP,
- AUDIO: Wejście sygnału audio stereo - zbalansowany i niezbalansowany, Wyjście sygnału audio "Talk-Back", 2 kanały audio przypadające na 1 kanał wideo Próbkowanie dla pary kanałów audio 32 do 384 kb/s, Częstotliwość kwantyzacji dla audio 48kHz, Kompresja audio - MPEG-2 AAC-LC , MPEG-4 AAC-LC, Embedowany cyfrowy sygnał audio SD-SDI : SMPTE-272M , HD-SDI:SMPTE-299M
- Wejście sygnału 3G-SDI, HD-SDI, SD-SDI, Composite, S-Video
- Sygnał 3G-SDI 1080p 50/60 fps video dla 3Gps
- Rozdzielczości wideo strumienia głównego: HD1080 - 1920X1080 - dla 1080p - 30/60 kl/s oraz 25/50 kl/s, dla 1080i - 30/25 kl/s, HD 720 - 1280X720 - dla 720p - 30/60 kl/s oraz 25/50 kl/s, SD 480 - 720X480 - dla 480i - 30 kl/s, SD 576 - 720X576 - dla 576i - 25 kl/s, Half-D1-PAL - 352x576 - dla 576i - 25kl/s, SIF - 352X288 - dla 480i - 30 kl/s , dla 576i - 25kl/s
- możliwość transmisji dwustrumieniowej (strumień w niższej rozdzielczości SD)

[C.7]	**Serwer dedykowany do systemu streamingu wideo**
Szafa serwerowa rack IT, 1 RU	

Serwer utrzymujący i zarządzający platformą transmisji sygnałów audio-wideo.

Parametry:

- Płyta główna wyposażona w układy bazowe czołowych producentów procesorów
- Procesor 1 x CPU min. 2.1 GHz,
- Pamięć operacyjna co najmniej 16 GB,
- Zintegrowana macierz dysków RAID-1 (2x1TB) 7.2K SATA 3.5" Hot-plug,
- LAN nie mniej niż 1 Gbit/s,
- Obudowa Rack 1U

4.1.18 Inne systemy

W obiekcie możliwe będzie instalowanie innych systemów podnoszących sprawność funkcjonowania i ekonomikę projektowanego szpitala

Część hotelową należy wyposażyć w system automatycznej recepcji hotelowej. System ma za zadanie wyeliminować konieczność obecności personelu recepcyjnego. Powinien umożliwiać dokonywania automatycznej rezerwacji pokoju, opcjonalną płatność zdalną lub na miejscu, realizacji automatycznego depozytu kluczy/kart dostępu do pokoi hotelowych, itp. Automat należy zainstalować w sekcji hotelowej w pom. komunikacji 5.113A. W automacie należy zaimplementować rozwiązania umożliwiające zdalną rezerwację pokoi (np. przez przeglądarkę internetową), rezerwację „na miejscu", płatności gotówką/kartą oraz inne wymagane przez Użytkownika. Część hotelową należy wyposażyć w kontrolę dostępu hotelową obsługującą ten sam standard kart jak dla budynkowego SKD. Umożliwi to unifikację kart stosowanych w obiekcie. Karty należy zaprogramować do odpowiednich pokoi hotelowych oraz do drzwi zewnętrznych części hotelowej objętej budynkowym SKD. Dostawca systemu automatycznej recepcji zobowiązany jest do przeszkolenia personelu w zakresie obsługi urządzenia, przygotowania instrukcji obsługi systemu, plansz graficznych ułatwiających obsługę urządzenia, itp.

4.1.19 Trasy kablowe

Projektuje się dedykowane trasy kablowe, których rozmieszczenia, szerokości oraz rzędne pokazano w części rysunkowej. Trasy kablowe niskoprądowe muszą być ulokowane z zachowaniem niezbędnych odstępów od pozostałych instalacji. Koryta muszą być wykonane z blachy o grubości minimum 1mm oraz wysokości ścianki bocznej 60mm

Koryta muszą mieć zachowaną ciągłość połączeń. W miejscach, gdzie wystąpi brak ciągłości, koryta należy łączyć linką PE Lg 6mm. System koryt kablowych powinien być kompletny i składać się z typowych elementów takich jak odcinki proste koryt, złącza, łuki, trójniki, wsporniki ścienne i sufitowe. Koryta będą mocowane do konstrukcji stropu i blachy trapezowej za pomocą zawiesi. Mając na uwadze delikatną budowę warstwy izolującej okablowanie należy zadbać o to, aby krawędzie koryt nie powodowały jej uszkodzenia. Koryta powinny być sztywne, a dystans miedzy wspornikami powinien zapewnić, że koryta nie będą skręcone (zwichrowane) lub wygięte. Powłokę galwaniczną uszkodzonych miejsc przecięcia korytek należy zabezpieczyć. Trasy głównych ciągów tras kablowych pokazano w części rysunkowej opracowania.

Na potrzeby systemów pożarowych należy zainstalować zespoły kablowe o cechach E90.

5 UWAGI

- Nieniejszy projekt stanowi wytyczną do wykonania i odbioru robót budowlanych kompletnego i w pełni funkcjonalnego szpitala. Brak wyszczególnienia jakiegokolwiek elementu, który może być zawarty w projekcie warsztatowym lub jest wymagany względami technologicznymi, aby skończone instalacje oraz budynek uznać za kompletny i zgodny z założeniami projektowymi, nie zwalnia Wykonawcy z obowiązku wykonania tych elementów i nie stanowi podstawy do rozszerzenia zakresu prac pomiędzy Inwestorem a Wykonawcą.
- Wszelkie elementy systemowe należy dobierać i wykonywać zgodnie z wytycznymi producenta oraz wymaganiami projektu. System należy stosować w sposób kompletny, wraz z wymaganymi zabezpieczeniami i akcesoriami. Niedopuszczalne jest stosowanie tylko wybranych elementów systemu, zastępowanie wybranych elementów nieoryginalnymi czy łączenie elementów z różnych systemów. Proponowane rozwiązania muszą uzyskać akceptację Inwestora i projektanta.
- Użytkownik wdroży procedury na wypadek sytuacji kryzysowych umożliwiające bezpieczną ewakuację i dokończenie procedur szpitalnych z uwzględnieniem przyjętych

rozwiązań technologicznych, np. procedurę bezpiecznego zakończenia operacji na wypadek alarmu pożarowego oraz procedurę bezpiecznego dla serwerów ich wyłączenia.

- Dokumentacja projektowa stanowi całość składającą się z części rysunkowej i opisowej i należy ją rozpatrywać łącznie, w tym z projektami branżowymi.
- Instalacje należy wykonywać zgodnie z wymaganiami przepisów i norm, w pierwszej kolejności zgodnie z rozporządzeniem Ministra Infrastruktury w sprawie „Warunków Technicznych, jakim powinny odpowiadać budynki i ich usytuowanie" – Dz. U. Nr 75, poz. 690 z 2002 roku z późniejszymi zmianami, następnie zgodnie z wymaganiami normy PN-IEC 60364 „Instalacje elektryczne w obiektach budowlanych".
- Wszystkie materiały i urządzenia stosowane przy budowie instalacji elektrycznych muszą posiadać znak CE, o ile wymaga tego Dyrektywa Budowlana, oraz muszą posiadać wymagane przez aktualne przepisy deklaracje lub certyfikaty zgodności z normami albo z aprobatami technicznymi.
- Przed zakupem materiałów i sprzętu na budowę uzyskać akceptację Inwestora.
- Przed zakupem materiałów, obmiarów należy dokonać bezpośrednio na budowie.
- Prace powinny być wykonane przez przeszkolonych instalatorów.
- Przy układaniu kabli, przewodów, zachować normatywne odległości pomiędzy kablami lub przewodami silnoprądowymi od przewodów niskoprądowych.
- Nigdy nie wolno przekraczać maksymalnych naciągów instalacyjnych kabli oraz promieni gięcia.
- Montaż i konserwacja sprzętu może zostać wykonana jedynie przez uprawnionych instalatorów posiadających stosowne dla danej instalacji szkolenia i certyfikaty wymagane prawem i przez producentów urządzeń.
- Przejścia przez przegrody budowlane należy uszczelnić zgodnie z klasą odporności pożarowej EI przegrody.
- Metalowe części szaf i skrzynek połączyć z systemem połączeń wyrównawczych.
- Rury kanalizacji teletechnicznej należy uszczelnić wodo- i gazoszczelnie.
- Przy prowadzeniu robót ziemnych należy zachować szczególną ostrożność w miejscach zbliżeń do istniejącego uzbrojenia podziemnego i naziemnego oraz budynków.
- Ostateczne lokalizacje głośników DSO należy skorygować na etapie realizacji do rzeczywistych warunków jakie będą panowały na obiekcie. Po dokonaniu pomiarów i prób, w razie konieczności należy dokonać korekt lokalizacji.
- Lokalizacje punktów WiFi oraz DECT należy skorygować na etapie realizacji do rzeczywistych warunków jakie będą panowały na obiekcie. Po dokonaniu pomiarów propagacji fal, w razie konieczności należy dokonać korekt lokalizacji.
- Lokalizacje kamer oraz regulacja ostatecznych kąta widzenia i pola zasięgu należy skorygować na etapie realizacji do rzeczywistych warunków jakie będą panowały na obiekcie. W razie konieczności należy dokonać korekt lokalizacji wg wytycznych Użytkownika oraz ochrony obiektu.

- Zgodnie z art. 21a Prawa Budowlanego, Kierownik Budowy jest zobowiązany sporządzić lub zapewnić sporządzenie przed rozpoczęciem budowy planu bezpieczeństwa i ochrony zdrowia.
- Przed rozpoczęciem robót instalacyjnych należy ustalać szczegółowe zasady ich prowadzenia z Inspektorem Nadzoru Inwestorskiego oraz uprawnionym użytkownikiem obiektu.
- Na terenie inwestycji mogą znajdować się niezidentyfikowane sieci teletechniczne. Prace należy prowadzić z zachowaniem szczególnej ostrożności. Istniejącą infrastrukturę należy zabezpieczyć przed uszkodzeniem.
- Przed oddaniem instalacji do eksploatacji należy wykonać wymagane przepisami i normami badania, próby i pomiary po montażowe.
- Po zakończeniu prac należy przekazać użytkownikowi dokumentację powykonawczą, plany i schematy z naniesionymi zmianami, protokoły badań oraz instrukcje obsługi i inne wymagane przez użytkownika dokumenty. Ilość egzemplarzy, zawartość dokumentów towarzyszących dokumentacji powykonawczej i ich formę należy ustalić przed rozpoczęciem prac.
- Całość robót wykonać według niniejszego opracowania zgodnie z wydanymi warunkami technicznymi, wymogami norm, rozwiązań typowych, przepisów budowy i bezpieczeństwa.

6 Klauzula dopuszczalności stosowania zamienników

Wszelkie nazwy własne produktów, materiałów i urządzeń przywołane w niniejszym projekcie należy traktować jako przykładowe, służące określeniu pożądanego standardu wykonania i określeniu niezbędnych właściwości i wymogów założonych w dokumentacji technicznej dla danych rozwiązań. Dopuszcza się zastąpienie proponowanych rozwiązań (w oparciu o wyroby innych producentów), pod warunkiem spełnienia określonych wymagań pod względem parametrów technicznych, funkcjonalnych i użytkowych wskazanych szczegółowo w dokumentacji projektowej.

7 Załączniki

7.1 Załącznik 1 – schemat połączeń ramach poszczególnych punktów dystrybucyjnych

7.2 Załącznik 2 – planowane pokrycie siecią bezprzewodową na poszczególnych piętrach szpitala

7.3 Załącznik 3 – zestawienie głośników DSO

7.4 Załącznik 4 – lista kablowa: system integracji sal operacyjnych

7.5 Załącznik 5 – lista kablowa: system integracji sal endoskopowych

7.6 Załącznik 6 – zestawienie materiałów systemu sygnalizacji pożaru SSP

7.7 Załącznik 7 – zestawienie materiałów dźwiękowego systemu ostrzegawczego DSO

7.8 Załącznik 8 – zestawienie sprzętu aktywnego LAN

7.9 Załącznik 9 – zestawienie elementów telefonii IP

7.10 Załącznik 10 – zestawienie elementów pasywnych sieci strukturalnej

7.11 Załącznik 11 – zestawienie elementów systemu kontroli dostępu skd

7.12 Załącznik 12 – zestawienie elementów systemu sygnalizacji włamania i napadu sswin

7.13 Załącznik 13 – zestawienie elementów systemu wideointerkomów

7.14 Załącznik 14 – zestawienie elementów systemu CCTV

7.15 Załącznik 15 – zestawienie elementów systemu bezpieczeństwa SMS

7.16 Załącznik 16 – zestawienie elementów systemu przyzywowego

7.17 Załącznik 17 – zestawienie elementów telefonii DECT

7.18 Załącznik 18 – zestawienie elementów systemu wykrywania gazów SWG

7.19 Załącznik 19 – zestawienie elementów instalacji RTV

7.20 Załącznik 20 – zestawienie elementów dla systemów AV

7.21 Załącznik 21 – zestawienie elementów systemu kolejkowego

7.22 Załącznik 22 – zestawienie elementów systemu integracji

7.23 Załącznik 23 – zestawienie elementów systemu tras kablowych

7.24 Załącznik 24 – zestawienie elementów systemu rejestracji czasu pracy RCP

8 Część rysunkowa