INDUSTRIA PROJECT Sp. z o.o.
80-298Gdańsk, 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

EGZEMPLARZ NR

Inwestor: **Uniwersytet Medyczny w Łodzi**, al. Kościuszki 4, 90-419 Łódź

Temat: **DRUGI ETAP BUDOWY CENTRUM KLINICZNO-DYDAKTYCZNEGO UNIWERSYTETU MEDYCZNEGO W ŁODZI WRAZ Z AKADEMICKIM OŚRODKIEM ONKOLOGICZNYM**

Adres: ul. Pomorska 251, 92-213 Łódź
dz. nr ewid. 411, obręb 106106_9.0014, W-14, jedn. ewid. ŁÓDŹ-WIDZEW

Kat. obiektu: IX, XI

Stadium: PROJEKT WYKONAWCZY

Nr projektu: IBG-P/240/18

Tom: **II – PROJEKT WYKONAWCZY - BUDYNKI A1, A2**

Część/Branża: VI – BRANŻA NISKOPRĄDOWA

BRANŻA	PROJEKTANT	PODPIS	SPRAWDZAJĄCY	PODPIS
NISKOPRĄDOWA	mgr inż. Radosław Markiewicz upr. nr POM/0002/POOT/09 w specjalności telekomunikacyjnej do projektowania bez ograniczeń		mgr inż. Jerzy Grubiak upr. nr POM/0175/PWOT/08 w specjalności telekomunikacyjnej do projektowania bez ograniczeń	
	inż. Marek Pobłocki upr. nr POM/0004/POOT/09 w specjalności telekomunikacyjnej do projektowania bez ograniczeń			

Gdańsk 07.2019

(pusta strona)

1 ZAWARTOŚĆ PROJEKTU

1.1 Spis kompletnej, wielobranżowej dokumentacji projektowej

SPIS ZAWARTOŚCI PROJEKTU WYKONAWCZEGO:

Tom I – FORMALNOŚCI

Część I	DOKUMENTY FORMALNO-PRAWNE
Część II	INFORMACJA DOTYCZĄCA BIOZ
Część III	ETAPOWANIE
Część IV	INSTRUKCJA EKSPLOATACJI BUDYNKÓW

Tom II – PROJEKT WYKONAWCZY - BUDYNKI A1, A2

Część I	ARCHITEKTURA
Część II	BRANŻA KONSTRUKCYJNA
Część III	BRANŻA SANITARNA
Część III.I	INSTALACJA WOD-KAN, KAN. DESZCZ., C.O. – BUDYNEK A1
Część III.II	INSTALACJA TRYSKACZOWA I HYDRANTOWA – BUDYNEK A1
Część III.III	WENTYLACJA, KLIMATYZACJA, INSTALACJA CHŁODNICZA I CIEPŁA TECHNOLOGICZNEGO – BUDYNEK A1
Część III.IV	WĘZEŁ CIEPLNY – BUDYNEK A1
Część III.V	INSTALACJA WOD-KAN, HYDRANTOWA, KAN. DESZCZ., C.O., GAZOWA – BUDYNEK A2
Część III.VI	WĘZEŁ CIEPLNY – BUDYNEK A2
Część III.VII	WENTYLACJA, KLIMATYZACJA, INSTALACJA CHŁODNICZA I CIEPŁA TECHNOLOGICZNEGO – BUDYNEK A2
Część IV	GAZY MEDYCZNE
Część V	BRANŻA ELEKTRYCZNA
Część VI	**BRANŻA NISKOPRĄDOWA**
Część VII	BRANŻA BMS
Część VIII	BRANŻA SUG
Część IX	OCHRONA RADIOLOGICZNA
Część X	TECHNOLOGIA MEDYCZNA Z LOGISTYKĄ
Część XI	INSTRUKCJA PPOŻ
Część XII	OPERAT AKUSTYCZNY

Tom III – PROJEKT WYKONAWCZY - STWIOR, PRZEDMIARY I KOSZTORYSY

Część I STWIOR

Część II PRZEDMIARY I KOSZTORYSY

1.2 Spis zawartości tomu II część VI – Branża Niskoprądowa

1.3 Spis części rysunkowej

L.p.	Nazwa rysunku	numer rysunku
	BUDYNEK A1	
1.	Rzut Poziomu 0 - System sygnalizacji pożaru - BUDYNEK A1	240-IP-A1-0-DR-N-65104
2.	Rzut Poziomu 3 - System sygnalizacji pożaru - BUDYNEK A1	240-IP-A1-3-DR-N-65107
3.	System Sygnalizacji Pożaru – schemat blokowy	240-IP-A1-XX-SD-N-65103
4.	Rzut Poziomu 0 - Dźwiękowy system ostrzegawczy - BUDYNEK A1	240-IP-A1-0-DR-N-64204
5.	Rzut Poziomu 3 - Dźwiękowy system ostrzegawczy - BUDYNEK A1	240-IP-A1-3-DR-N-64207
6.	Dźwiękowy System Ostrzegawczy DSO – schemat strukturalny systemu	240-IP-A1-XX-SD-N-64201
7.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO1	240-IP-A1-XX-SD-N-64202
8.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO2	240-IP-A1-XX-SD-N-64203
9.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO3	240-IP-A1-XX-SD-N-64204
10.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO4	240-IP-A1-XX-SD-N-64205
11.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO5	240-IP-A1-XX-SD-N-64206
12.	Rzut Poziomu 0 – System Kontroli Dostępu - BUDYNEK A1	240-IP-A1-0-DR-N-64104
13.	Rzut Poziomu 3 – System Kontroli Dostępu - BUDYNEK A1	240-IP-A1-3-DR-N-64106
14.	System Kontroli Dostępu – schemat blokowy – BUDYNEK A1	240-IP-A1-XX-SD-N-64101
15.	Rzut poziomu 0 - LAN i Access Point - BUDYNEK A1	240-IP-A1-0-DR-N-64404
16.	Rzut poziomu 3 - LAN i Access Point - BUDYNEK A1	240-IP-A1-3-DR-N-64407
17.	System okablowania strukturalnego – schemat blokowy	240-IP-A1-XX-SD-N-64401
18.	Rzut Poziomu 0 – System Telewizji Dozorowej - BUDYNEK A1	240-IP-A1-0-DR-N-64302
19.	Rzut Poziomu 3 – System Telewizji Dozorowej - BUDYNEK A1	240-IP-A1-3-DR-N-64304
20.	Rzut Poziomu 0 – System Sygnalizacji Włamania i Napadu – BUDYNEK A1	240-IP-A1-0-DR-N-65202
21.	Rzut Poziomu 3 – System Sygnalizacji Włamania i Napadu – BUDYNEK A1	240-IP-A1-3-DR-N-65203
22.	System Sygnalizacji Włamania i Napadu – schemat blokowy	240-IP-A1-XX-SD-N-65201
23.	Rzut Poziomu 0 - Instalacja Przyzywowa - BUDYNEK A1	240-IP-A1-0-DR-N-65301
24.	Rzut Poziomu 3 - Instalacja Przyzywowa - BUDYNEK A1	240-IP-A1-3-DR-N-65303
25.	Rzut Poziomu 0 - Instalacja Przyzywowa – schemat blokowy	240-IP-A1-0-SD-N-65302
26.	Rzut Poziomu 3 - Instalacja Przyzywowa – schemat blokowy	240-IP-A1-3-SD-N-65304
27.	Rzut Poziomu 0 - System audio-wizualny - BUDYNEK A1	240-IP-A1-0-DR-N-64501
28.	Rzut Poziomu 3 - System audio-wizualny - BUDYNEK A1	240-IP-A1-3-DR-N-64503
29.	System AV – schemat ideowy dla standardu 1	240-IP-A1-XX-SD-N-64501
30.	Rzut Poziomu 0 – Plan tras kablowych – BUDYNEK A1	240-IP-A1-0-DR-N-64704
31.	Rzut Poziomu 3 – Plan tras kablowych – BUDYNEK A1	240-IP-A1-3-DR-N-64707
32.	System Wykrywania Gazu – schemat blokowy – BUDYNEK A1	240-IP-A1-XX-SD-N-65501
33.	Rzut Poziomu 02 – LAN i Access Point – BUDYNEK A2 – część 1	240-IP-A2-02-DR-N-64401
34.	Rzut Poziomu 02 – LAN i Access Point – BUDYNEK A2 – część 2	240-IP-A2-02-DR-N-64402
35.	Rzut Poziomu 01 – LAN i Access Point – BUDYNEK A2 – część 1	240-IP-A2-01-DR-N-64403
36.	Rzut Poziomu 01 – LAN i Access Point – BUDYNEK A2 – część 2	240-IP-A2-01-DR-N-64404
37.	Rzut Poziomu 0 – LAN i Access Point – BUDYNEK A2 – część 1	240-IP-A2-0-DR-N-64405

38.	Rzut Poziomu 0 – LAN i Access Point – BUDYNEK A2 – część 2	240-IP-A2-0-DR-N-64406
39.	Rzut Poziomu 1 – LAN i Access Point – BUDYNEK A2 – część 1	240-IP-A2-1-DR-N-64407
40.	Rzut Poziomu 1 – LAN i Access Point – BUDYNEK A2 – część 2	240-IP-A2-1-DR-N-64408
41.	System Okablowania Strukturalnego – schemat blokowy – BUDYNEK A2	240-IP-A2-XX-SD-N-64401
42.	Rzut Poziomu 02 – Systemy SSP i Oddymiania – BUDYNEK A2 – część 1	240-IP-A2-02-DR-N-65101
43.	Rzut Poziomu 02 – Systemy SSP i Oddymiania – BUDYNEK A2 – część 2	240-IP-A2-02-DR-N-65102
44.	Rzut Poziomu 01 – Systemy SSP i Oddymiania – BUDYNEK A2 – część 1	240-IP-A2-01-DR-N-65103
45.	Rzut Poziomu 01 – Systemy SSP i Oddymiania – BUDYNEK A2 – część 2	240-IP-A2-01-DR-N-65104
46.	Rzut Poziomu 0 – Systemy SSP i Oddymiania – BUDYNEK A2 – część 1	240-IP-A2-0-DR-N-65105
47.	Rzut Poziomu 0 – Systemy SSP i Oddymiania – BUDYNEK A2 – część 2	240-IP-A2-0-DR-N-65106
48.	Rzut Poziomu 1 – Systemy SSP i Oddymiania – BUDYNEK A2 – część 1	240-IP-A2-1-DR-N-65107
49.	Rzut Poziomu 1 – Systemy SSP i Oddymiania – BUDYNEK A2 – część 2	240-IP-A2-1-DR-N-65108
50.	Schemat ideowy Systemu Sygnalizacji Pożarowej pracującego w sieci „Integral WAN”	240-IP-A2-XX-SD-N-65101
51.	Instalacja oddymiania – schemat blokowy – BUDYNEK A2	240-IP-A2-XX-SD-N-65102
52.	System Sygnalizacji Pożaru – schemat blokowy – BUDYNEK A2	240-IP-A2-XX-SD-N-65103
53.	Rzut Poziomu 02 – Dźwiękowy system ostrzegawczy – BUDYNEK A2 – część 1	240-IP-A2-02-DR-N-64201
54.	Rzut Poziomu 02 – Dźwiękowy system ostrzegawczy – BUDYNEK A2 – część 2	240-IP-A2-02-DR-N-64202
55.	Rzut Poziomu 01 – Dźwiękowy system ostrzegawczy – BUDYNEK A2 – część 1	240-IP-A2-01-DR-N-64203
56.	Rzut Poziomu 01 – Dźwiękowy system ostrzegawczy – BUDYNEK A2 – część 2	240-IP-A2-01-DR-N-64204
57.	Rzut Poziomu 0 – Dźwiękowy system ostrzegawczy – BUDYNEK A2 – część 1	240-IP-A2-0-DR-N-64205
58.	Rzut Poziomu 0 – Dźwiękowy system ostrzegawczy – BUDYNEK A2 – część 2	240-IP-A2-0-DR-N-64206
59.	Rzut Poziomu 1 – Dźwiękowy system ostrzegawczy – BUDYNEK A2 – część 1	240-IP-A2-1-DR-N-64207
60.	Rzut Poziomu 1 – Dźwiękowy system ostrzegawczy – BUDYNEK A2 – część 2	240-IP-A2-1-DR-N-64208
61.	Dźwiękowy System Ostrzegawczy DSO – schemat strukturalny systemu – BYDYNEK A2	240-IP-A2-XX-SD-N-64201
62.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO1	240-IP-A2-XX-SD-N-64202
63.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO2	240-IP-A2-XX-SD-N-64203
64.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO3	240-IP-A2-XX-SD-N-64204
65.	Dźwiękowy System Ostrzegawczy DSO – schemat szafy CDSO4	240-IP-A2-XX-SD-N-64205
66.	Rzut Poziomu 02 – System Kontroli Dostępu – BUDYNEK A2	240-IP-A2-02-DR-N-64101
67.	Rzut Poziomu 01 – System Kontroli Dostępu – BUDYNEK A2	240-IP-A2-01-DR-N-64102
68.	Rzut Poziomu 0 – System Kontroli Dostępu – BUDYNEK A2	240-IP-A2-0-DR-N-64103
69.	Rzut Poziomu 1 – System Kontroli Dostępu – BUDYNEK A2	240-IP-A2-1-DR-N-64104
70.	Schemat blokowy poziomu 02 – System Kontroli Dostępu – BUDYNEK A2	240-IP-A2-02-SD-N-64101
71.	Schemat blokowy poziomu 01 – System Kontroli Dostępu – BUDYNEK A2	240-IP-A2-01-SD-N-64102
72.	Schemat blokowy poziomu 0 – System Kontroli Dostępu – BUDYNEK A2	240-IP-A2-0-SD-N-64103
73.	Schemat blokowy poziomu 1 – System Kontroli Dostępu – BUDYNEK A2	240-IP-A2-1-SD-N-64104
74.	Rzut Poziomu 02 – System Telewizji Dozorowej – BUDYNEK A2	240-IP-A2-02-DR-N-64301
75.	Rzut Poziomu 01 – System Telewizji Dozorowej – BUDYNEK A2	240-IP-A2-01-DR-N-64302
76.	Rzut Poziomu 0 – System Telewizji Dozorowej – BUDYNEK A2	240-IP-A2-0-DR-N-64303
77.	Rzut Poziomu 1 – System Telewizji Dozorowej – BUDYNEK A2	240-IP-A2-1-DR-N-64304
78.	System Telewizji Dozorowej – schemat blokowy	240-IP-XX-XX-SD-N-64301
79.	Rzut Poziomu 02 – Instalacja przyzywowa – BUDYNEK A2	240-IP-A2-02-DR-N-65300
80.	Rzut Poziomu 01 – Instalacja przyzywowa – BUDYNEK A2	240-IP-A2-01-DR-N-65301
81.	Rzut Poziomu 0 – Instalacja przyzywowa – BUDYNEK A2	240-IP-A2-0-DR-N-65302

82.	Rzut Poziomu 1 – Instalacja przyzywowa – BUDYNEK A2	240-IP-A2-1-DR-N-65303
83.	Rzut Poziomu 02 – Instalacja przyzywowa – schemat blokowy	240-IP-A2-02-SD-N-65301
84.	Rzut Poziomu 01 – Instalacja przyzywowa – schemat blokowy	240-IP-A2-01-SD-N-65302
85.	Rzut Poziomu 0 – Instalacja przyzywowa – schemat blokowy	240-IP-A2-0-SD-N-65303
86.	Rzut Poziomu 1 – Instalacja przyzywowa – schemat blokowy	240-IP-A2-1-SD-N-65304
87.	Rzut Poziomu 02 – System audio-wizualny – BUDYNEK A2	240-IP-A2-02-DR-N-64501
88.	Rzut Poziomu 01 – System audio-wizualny – BUDYNEK A2	240-IP-A2-01-DR-N-64502
89.	Rzut Poziomu 0 – System audio-wizualny – BUDYNEK A2	240-IP-A2-0-DR-N-64503
90.	Rzut Poziomu 1 – System audio-wizualny – BUDYNEK A2	240-IP-A2-1-DR-N-64504
91.	System AV – schemat ideowy dla standardu 1	240-IP-A2-XX-SD-N-64501
92.	System AV – schemat ideowy dla standardu 2	240-IP-A2-XX-SD-N-64502
93.	System AV – schemat ideowy dla standardu 3	240-IP-A2-XX-SD-N-64503
94.	System AV – schemat ideowy dla standardu 4	240-IP-A2-XX-SD-N-64504
95.	System AV – szafa AV standardu 4	240-IP-A2-XX-SD-N-64505
96.	System AV – wyposażenie rozdzielnicy dla standardu 4	240-IP-A2-XX-SD-N-64506
97.	Rzut Poziomu 02 – System Sygnalizacji Włamania i Napadu – BUDYNEK A2	240-IP-A2-02-DR-N-65201
98.	Rzut Poziomu 01 – System Sygnalizacji Włamania i Napadu – BUDYNEK A2	240-IP-A2-01-DR-N-65202
99.	Rzut Poziomu 00 – System Sygnalizacji Włamania i Napadu – BUDYNEK A2 – część 1	240-IP-A2-0-DR-N-65203
100.	Rzut Poziomu 00 – System Sygnalizacji Włamania i Napadu – BUDYNEK A2 – część 2	240-IP-A2-0-DR-N-65204
101.	Rzut Poziomu 1 – System Sygnalizacji Włamania i Napadu – BUDYNEK A2	240-IP-A2-1-DR-N-65205
102.	System Sygnalizacji Włamania i Napadu – schemat blokowy	240-IP-A2-XX-SD-N-65201
103.	Rzut Poziomu 02 – Plan tras kablowych – BUDYNEK A2 – część 1	240-IP-A2-02-DR-N-64701
104.	Rzut Poziomu 02 – Plan tras kablowych – BUDYNEK A2 – część 2	240-IP-A2-02-DR-N-64702
105.	Rzut Poziomu 01 – Plan tras kablowych – BUDYNEK A2 – część 1	240-IP-A2-01-DR-N-64703
106.	Rzut Poziomu 01 – Plan tras kablowych – BUDYNEK A2 – część 2	240-IP-A2-01-DR-N-64704
107.	Rzut Poziomu 0 – Plan tras kablowych – BUDYNEK A2 – część 1	240-IP-A2-0-DR-N-64705
108.	Rzut Poziomu 0 – Plan tras kablowych – BUDYNEK A2 – część 2	240-IP-A2-0-DR-N-64706
109.	Rzut Poziomu 1 – Plan tras kablowych – BUDYNEK A2 – część 1	240-IP-A2-1-DR-N-64707
110.	Rzut Poziomu 1 – Plan tras kablowych – BUDYNEK A2 – część 2	240-IP-A2-1-DR-N-64708
111.	Rzut Poziomu 02 – System Wykrywania Gazu – BUDYNEK A2	240-IP-A2-02-DR-N-65501
112.	Rzut Poziomu 01 – System Wykrywania Gazu – BUDYNEK A2	240-IP-A2-01-DR-N-65502
113.	System Wykrywania Gazu – schemat blokowy – BUDYNEK A2	240-IP-A2-XX-SD-N-65501
	BUDYNEK A1 i A2	
114.	System zliczania osób – schemat blokowy	240-IP-00-XX-SD-N-64001

2 PODZIAŁ NA ETAPY I PODETAPY (FAZY) DLA PROJEKTU WYKONAWCZEGO

Podział projektu wykonawczego, w zakresie branży ARCHITEKTURA, obejmującego części budynków A1 i A2 nieobjęte etapami I-V, przewidziane do realizacji w etapie VI, określonym w decyzji nr DAR-UA-II.1775.2012 z dnia 18.12.2012 r., z którego wyodrębnia się etapy:

- Etap VII – obejmujący zmianę zamierzonego sposobu użytkowania części budynku A1, w osiach 1÷28/J'''÷K''', na zespół oddziałów specjalistycznych, pracownię specjalistyczną, hostel specjalistyczny, szatnie i magazyny, pomieszczenia techniczne i komunikację, z podziałem na podetapy wymienione poniżej;
- Etap VIII – obejmujący zmianę zamierzonego sposobu użytkowania części budynku A2, w osiach 9'÷18/F÷J'' w części A-2-1 oraz w osiach 1'÷27/A'÷J'' w *części* A-2-2, na: zespół oddziałów specjalistycznych, poradni specjalistycznych, pracowni specjalistycznych, laboratoria, pomieszczenia: izby przyjęć, bloku operacyjnego, centralnej sterylizatorni, banku krwi, apteki, podstawowej opieki zdrowotnej, administracji, relaksu, szatnie i magazyny, pomieszczenia techniczne i komunikację, z podziałem na podetapy wymienione poniżej.

W załącznikach graficznych nr od 240-IP-00-03-SD-A-00001 do 240-IP-00-17-SD-A-00021, obejmujących 21 kondygnacji szpitala, został przedstawiony schemat etapowania, w podziale na stan realizacji :

- Zrealizowane – Etap I, II, III, IV,

- W trakcie realizacji – Etap VI,

- Niezrealizowane - Etap V,

- Objęte niniejszym opracowaniem – **Etap VII** i **VIII**.

ETAP VII → BUDYNEK A1

obejmuje:

- BUDYNEK A1 – POZIOMY OD 03 DO 17 (Z WYŁĄCZENIEM KONDYGNACJI 01)

(03,02 - kondygnacje podziemne, kondygnacje nadziemne 01, 0, 1…17)

Każdy Etap został odpowiednio podzielony na Podetapy realizacji zwane dalej Fazami.
Przewidziano podział faz na odpowiednio:
a – zagospodarowanie pustostanów szpitala,
b – przebudowa istniejących jednostek szpitala .
Poniżej przedstawiony został opis poszczególnych jednostek za pomocą osi konstrukcyjnych oraz przypisane mu odpowiednie Podetapy/Fazy.

- Podetap VII-0 (Faza 0): poziom 03 (piwnica -1) w osiach 1÷8/J'''÷K''' oraz poziom 17 (18 piętro) w osiach 1''÷8/J''÷K'', 8÷10/J''÷K – pomieszczenia techniczne i komunikacja.
- Podetap VII-1a (Faza 1a): poziom 16 (17 piętro) w osiach 16'÷25/J''÷K'' – Oddział Neonatologii.
- Podetap VII-2a (Faza 2a): poziom 16 (17 piętro) w osiach 1'''÷16'/J''÷K'' – Oddział Położniczy z blokiem porodowym.
- Podetap VII-3a (Faza 3a): poziom 15 (16 piętro) w osiach 18÷25/J''÷K'' – Oddział Endokrynologii.

- Podetap VII-4a (Faza 4a): poziom 15 (16 piętro) w osiach 10÷18/J''÷K'' – Oddział Chemioterapii.
- Podetap VII-5a (Faza 5a): poziom 15 (16 piętro) w osiach 1'''÷10/J''÷K'' – Oddział Onkologii Ogólnej.
- Podetap VII-6a (Faza 6a): poziom 13 (14 piętro) w osiach 1'''÷8/J''÷K'' – Hostel Onkologiczny.
- Podetap VII-7a (Faza 7a): poziom 11 (12 piętro) w osiach 16'÷25/J''÷K'' – Oddział Neurologii.
- Podetap VII-8a (Faza 8a): poziom 11 (12 piętro) w osiach 8÷16'/J''÷K'' – Oddział Neurochirurgii.
- Podetap VII-9a (Faza 9a): poziom 11 (12 piętro) w osiach 1'''÷8/J''÷K'' – Oddział Geriatryczny.
- Podetap VII-10a (Faza 10a): poziom 10 (11 piętro) w osiach 1'''÷25/J''÷K'' – Oddział Chirurgii Onkologicznej.
- Podetap VII-11a (Faza 11a): poziom 9 (10 piętro) w osiach 1'''÷8/J''÷K'' – Pracownia Histopatologii.
- Podetap VII-12a (Faza 12a): poziom 8 (9 piętro) w osiach 1'''÷8/J''÷K'' – Oddział Medycyny Paliatywnej.
- Podetap VII-13a (Faza 13a): poziom 7 (8 piętro) w osiach 1'''÷8/J''÷K'' – Oddział Urologii.
- Podetap VII-14a (Faza 14a): poziom 6 (7 piętro) w osiach 1'''÷8/J''÷K'' – Oddział Ginekologii Onkologicznej.
- Podetap VII-15a (Faza 15a): poziom 3 (4 piętro) w osiach 1'''÷8/J''÷K'' – Oddział Radioterapii.
- Podetap VII-16a (Faza 16a): poziom 0 (1 piętro) w osiach 1÷10/H÷K'' – Oddział Chemioterapii Dziennej.
- Podetap VII-17a (Faza 17a): poziom 02 (piwnica) w osiach 1÷9/L÷K''' – Szatnie i magazyny, pomieszczenia techniczne i komunikacja.
- Podetap VII-18a (Faza 18a): poziom 12 (13 piętro) w osiach 1'''÷8/J''÷K'' – Centrum Symulacji Medycznych.
- Podetap VII-19a (Faza 19a): poziom 14 (15 piętro) w osiach 1'''÷10/J''÷K'' – Oddział Pediatrii i Hematologii.
- Podetap VII-20a (Faza 20a): poziom 14 (15 piętro) w osiach 10÷16'/J''÷K'' – Oddział Leczenia Jednego Dnia Onkohematologii Dziecięcej z odcinkiem transplantologicznym.
- Podetap VII-21a (Faza 21a): poziom 14 (15 piętro) w osiach 16'÷25/J''÷K'' – Oddział Pediatrii i Onkologii.
- Podetap VII-22a (Faza 22a): poziom 5 (6 piętro) w osiach 1'''÷8/J''÷K'' – Oddział Elektrokardiologii.
- Podetap VII-23a (Faza 23a): poziom 4 (5 piętro) w osiach 1'''÷8/J''÷K'' – Oddział Kardiologii Dziecięcej.
- Podetap VII-24a (Faza 24a): poziom 1 (2 piętro) w osiach 1'''÷8/J''÷K'' – Oddział Chirurgii Naczyniowej.

ETAP VIII → BUDYNEK A2

obejmuje:

- BUDYNEK A2 – POZIOMY OD 02 DO 1

(02 - kondygnacja podziemna, kondygnacje nadziemne 01, 0, 1)

Każdy Etap został odpowiednio podzielony na Podetapy realizacji zwane dalej Fazami.
Przewidziano podział faz na odpowiednio:

a – zagospodarowanie pustostanów szpitala,
b – przebudowa istniejących jednostek szpitala .
Poniżej przedstawiony został opis poszczególnych jednostek za pomocą osi konstrukcyjnych oraz przypisane mu odpowiednie Podetapy/Fazy.

- Podetap VIII-0 (Faza 0): poziom 02 (piwnica) w osiach 8÷10'/D÷J', 10'÷16'/K÷J', 13÷18/D÷D' – pomieszczenia techniczne i komunikacja.
- Podetap VIII-1a (Faza 1a): poziom 0 (1 piętro) w osiach 10'÷25'/A÷F – Izba Przyjęć.
- Podetap VIII-2a (Faza 2a): poziom 02 (piwnica) w osiach 19÷27/D÷H – Laboratoria diagnostyczne.
- Podetap VIII-3a/b (Faza 3a/b): poziom 01 (parter) w osiach 9'÷22/C÷J'' – Blok Operacyjny z salą wybudzeń.
- Podetap VIII-4a (Faza 4a): poziom 02 (piwnica) w osiach 10÷18/D÷F – Centralna Sterylizatornia.
- Podetap VIII-5a (Faza 5a): poziom 02 (piwnica) w osiach 18÷19/D÷F – Bank Krwi.
- Podetap VIII-6b (Faza 6b): poziom 02 (piwnica) w osiach 9'÷18'/F÷J' oraz poziom 1 (2 piętro) w osiach 10÷18'/F'÷J'' – Apteka z pracownią cytostatyczną.
- Podetap VIII-7a (Faza 7a): poziom 1 (2 piętro) w osiach 1'÷10/A'÷F – Poradnie.
- Podetap VIII-8b (Faza 8b): poziom 1 (2 piętro) w osiach 9'÷10/F÷J'' – Pracownia Immunopatologii i Genetyki.
- Podetap VIII-9a (Faza 9a): poziom 0 (1 piętro) w osiach 2÷10'/B÷F – Poradnie.
- Podetap VIII-10b (Faza 10b): poziom 0 (1 piętro) w osiach 9'÷10/F÷J'' – Centrum Opieki Koordynowanej.
- Podetap VIII-11a (Faza 11a): poziom 02 (piwnica) w osiach 1÷2/A÷D, 2÷27/C÷D, 25'÷27/D÷F – Szatnie i magazyny.
- Podetap VIII-12a (Faza 12a): poziom 0 (1 piętro) w osiach 25'÷27/H÷J' – Oddział Anestezjologii i Intensywnej Terapii.
- Podetap VIII-13a (Faza 13a): poziom 0 (1 piętro) w osiach 17'÷22/E÷G – Pracownia Hemodynamiki przy Izbie Przyjęć.
- Podetap VIII-14b (Faza 14a): poziom 0 (1 piętro) w osiach 17÷18'/F÷J' – Centrum Badań Klinicznych.
- Podetap VIII-15b (Faza 15b): poziom 0 (1 piętro) w osiach 16÷17/G÷G' – Pracownia Pediatrycznej Opieki Paliatywnej.
- Podetap VIII-16b (Faza 16b): poziom 0 (1 piętro) w osiach 10÷17'/G÷H – Oddział Polisomnografii.
- Podetap VIII-17a (Faza 17a): poziom 01 (parter) w osiach 21÷27/C÷F – Oddział Endoskopii i Chirurgii jednego Dnia.
- Podetap VIII-18a (Faza 18a): poziom 01 (parter) w osiach 1÷2/A÷D, 9'÷18/B÷C – Strefa Relaksu Studentów.
- Podetap VIII-19a (Faza 19a): poziom 01 (parter) w osiach 2÷9'/C÷D – POZ (Podstawowa Opieka Zdrowotna).
- Podetap VIII-20a (Faza 20a): poziom 1 (2 piętro) w osiach 16÷27/B3÷H – Administracja Szpitalna.
- Podetap VIII-21a (Faza 21a): poziom 1 (2 piętro) w osiach 10÷16/B3÷F' – Brain.

– Podetap VIII-22a (Faza 22a): poziom 01 (parter) w osiach 24÷27/F÷H oraz poziom 0 (1 piętro) w osiach 24÷27/F÷H – Toksykologia.

Etapowanie nie obejmuje części zamierzenia budowlanego zrealizowanej i oddanej do użytkowania.

3 DOKUMENTY POWIĄZANE

3.1 Podstawa opracowania

- Umowa na wykonanie prac projektowych,
- Koncepcja Programowo-przestrzenna rozbudowy i przebudowy istniejącego budynku szpitala
- Uzgodnienia z zakresu ochrony p.poż., BHP, warunków higieniczno-sanitarnych,
- 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,

- Rozporządzenia Ministra Zdrowia z dnia 26 czerwca 2012 w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą (Dz.U. 2012 poz. 739),
- Rozporządzenie Ministra Zdrowia z dnia 21 sierpnia 2006 w sprawie szczegółowych warunków bezpiecznej pracy z urządzeniami radiologicznymi (Dz. U. Nr 180, poz. 1325),
- Rozporządzenie Ministra Zdrowia z dnia 12 lipca 2006 w sprawie szczegółowych warunków bezpiecznej pracy ze źródłami promieniowania jonizującego (Dz.U. 2006 nr 140 poz. 994),
- Obowiązujące normy, m.in. PN-EN 54, CE-TS 54-32,
- Wytyczne projektowania instalacji sygnalizacji pożarowej SITP WP-02:2010,
- PN-EN 50173-1:2009/A1:2010 Technika Informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne
- PN-EN 50173-2:2008 Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Budynki biurowe;
- PN-EN 50174-1:2009 Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja i zapewnienie jakości;
- PN-EN 50174-2:2009 Technika informatyczna. Instalacja okablowania – Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków;
- PN-EN 50174-3:2005 Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków;
- PN-EN 50346:2004/A2:2010 - Technika informatyczna -Instalacja okablowania - Badanie zainstalowanego okablowania
- PN-EN 50131 Systemy alarmowe - Systemy sygnalizacji włamania,
- PN-EN 50132 Systemy alarmowe - Systemy dozorowe CCTV,
- PN-EN 50133 Systemy alarmowe - Systemy kontroli dostępu,
- Program Funkcjonalno Użytkowy oraz opracowanie koncepcyjne,
- Aktualne normy i rozporządzenia
- Zasady wiedzy technicznej.

4 DANE OGÓLNE

4.1 Przedmiot inwestycji i zakres opracowania

Przedmiotem inwestycji jest projekt budowlany rozbudowy budynku A1 i A2 oraz wózkowni wraz z łącznikiem C8 Centrum Kliniczno-Dydaktycznego Uniwersytetu Medycznego w Łodzi. Zakresem opracowania jest dostosowanie istniejącej niezagospodarowanej części budynków do nowego programu medycznego.

4.2 Cel opracowania

Celem opracowania jest przygotowanie projektu budowlanego dla wieloletniej inwestycji pn. „DRUGI ETAP BUDOWY CENTRUM KLINICZNO-DYDAKTYCZNEGO UNIWERSYTETU MEDYCZNEGO W ŁODZI WRAZ Z AKADEMICKIM OŚRODKIEM ONKOLOGICZNYM" prowadzonej przez Uniwersytet Medyczny w Łodzi oraz z przygotowanie niezbędnych materiałów potrzebnych do uzyskania decyzji o pozwoleniu na budowę.

4.3 Lokalizacja i przeznaczenie inwestycji

Przedmiotowa inwestycja usytuowana jest w Łodzi przy ul. Pomorskiej 251 na działce nr ewid. 411, obręb 106106_9.0014, W-14, jedn. ewid. ŁÓDŹ-WIDZEW.

Nowy program medyczny realizowany w budynku A1 i A2 będzie przeznaczony do prowadzenia działalności leczniczej.

Dokładna lokalizacja, projektowane zagospodarowanie terenu oraz zakres opracowania zostały przedstawione w części opisowej i rysunkowej w dokumentacji: TOM II – BUDYNKI A1 i A2, WÓZKOWNI WRAZ Z ŁĄCZNIKIEM C8.

5 OPIS TECHNICZNY

5.1 System Sygnalizacji Pożaru

Zakres realizacji

Na potrzeby obszarów objętych zakresem niniejszego opracowania projektuje się System Sygnalizacji Pożaru w oparciu o urządzenia kompatybilne z zainstalowanym systemem w istniejącej części Szpitala. Projektuje się system central rozproszonych po budynkach A1 oraz A2, zostaną one połączone z istniejącą na obiekcie siecią central „Integral WAN".
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).
Projektuje się ochronę pełną obiektu, chronione nie będą wybrane pomieszczenia niewymagające ochrony (np. sanitariaty).
Zadaniem Systemu Sygnalizacji Pożaru będzie:

- sygnalizowanie o źródle pożaru, wykrytym przez współpracujące czujki pożarowe oraz ręczne ostrzegacze pożarowe do głównej centrali SSP w istniejącej części szpitala,
- 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 wind na zjazd na poziom ewakuacyjny;
- zwolnienie przejść na drogach ewakuacyjnych objętych SKD;
- wysterowanie i monitorowanie systemu oddymiania i napowietrzania;
- monitorowanie systemu oddymiania grawitacyjnego w budynku A2,
- monitorowanie zasilaczy pożarowych;
- automatyczne przekazywanie sygnału o alarmie II stopnia do centrali głównej;
- wysterowanie i monitorowanie instalacji tryskaczowej;
- 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.
Zakres pomieszczeń objętych systemem oraz lokalizacje Ręcznych Ostrzegaczy Pożarowych i centrali pożarowej wraz z schematem blokowym pokazano w części rysunkowej projektu.

Sieć central sygnalizacji pożarowej

Centrale sygnalizacji pożarowej i sterowania urządzeniami ppoż będą połączone w sieć o topologii redundantnych pierścieni z wykorzystaniem przewodów miedzianych PH90. W układzie podstawowym system musi umożliwiać podłączenie około 50 central, zapewniając tym podłączenie istniejących i nowo zaprojektowanych central a także zapewniając minimalny zapas do przyszłej rozbudowy.

Opis systemu

Projektuje się instalację adresowalną opartą na centralach, które zostaną zainstalowane w wydzielonych pożarowo pomieszczeniach teletechnicznych oraz w punktach ochrony.
Automatyczna detekcja dymu realizowana będzie głównie za pomocą punktowych optycznych czujek dymu, a 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 połączeniu z zadziałaniem czujki.
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.
Na potrzeby wykonania połączenia pomiędzy projektowanymi a istniejącą siecią central należy wyposażyć je w dedykowane moduły komunikacyjne i niezbędne interfejsy, a następnie przeprowadzić niezbędne programowanie i uruchomienie systemu.

Zasilanie centrali i zasilaczy pożarowych

Centralę 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 centrali 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 należy obliczać korzystając ze wzoru:

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

gdzie:

Q	pojemność akumulatora [Ah]
k	współczynnik bezpieczeństwa
I_{CZ}	prąd czuwania [A]

I_A prąd alarmowania [A]

t_{CZ} czas czuwania [h]

t_A czas alarmowania [h]

lub korzystając z dedykowanego kalkulatora producenta systemu SSP.

Zestaw zasilacza z akumulatorami przejmie zasilanie systemu zaraz po zarejestrowaniu przerwy w dostawie prądu z sieci zasilającej. W przypadku znacznej pojemności baterii akumulatorów dedykowanych dla centrali SSP należy przewidzieć dodatkowe obudowy i moduły zasilające systemu SSP pozwalające na doładowanie akumulatorów w określonym normą czasie.

Algorytm sterowań

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. Wyjątkiem jest wciśnięcie przycisku ROP w pomieszczeniu ochrony przy centrali – wywołuje ono bezzwłocznie alarm II stopnia.

Po zadziałaniu elementu wykrywczego centrala będzie sygnalizować ALARM I STOPNIA lub ALARM II STOPNIA w zależności od rodzaju elementu wykrywczego oraz zaprogramowanych trybów alarmowania.

ALARM I STOPNIA sygnalizowany będzie przez centrale SSP. Jest to alarm wewnętrzny (tzw. cichy) i wymaga rozpoznania sytuacji przez dyżurujący personel. Nie powoduje on transmisji do PSP. Obsługa w czasie T1 - około 1 minuty potwierdza wystąpienie alarmu. Jeżeli tego nie zrobi, centrala wchodzi w ALARM II STOPNIA. Jeżeli natomiast nastąpi potwierdzenie alarmu, wówczas obsługa ma czas T2 - około 3 minuty na rozpoznanie zagrożenia pożarowego.

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.

Algorytm dla pożaru powstałego w pomieszczeniu szpitalnym

Z chwilą odebrania sygnału w centrali systemu sygnalizacji pożaru, opisane poniżej działania są wykonane automatycznie lub ręcznie przez pracowników ochrony.

Zasygnalizowanie na tablicy centrali pożarowej sygnału alarmu pożarowego.

Zadziałanie sygnalizatorów optycznych w strefie, w której system wykrył pożar.

Źródło informacji: czujka systemu sygnalizacji pożaru.

Automatyczne zadziałanie alarmu ograniczonego w centrali pożarowej – alarm I stopnia (czas trwania tego stanu jest ograniczony do 3 minut).

Sprawdzenie na miejscu źródła sygnału przez pracownika ochrony.

1. w przypadku drobnego incydentu: ręczna kasacja stanu alarmowanie i przestawienie centrali pożarowej na czuwanie,
2. w przypadku poważnego zagrożenia pożarowego - ręczne uruchomienie najbliżej położonego ROP – aktywacja alarmu II stopnia,
3. w przypadku braku reakcji po 3 minutach automatyczna aktywacja alarmu II stopnia,

Alarm II stopnia powoduje uruchomienie następującej sekwencji zdarzeń:

- ⇨ przekazanie sygnału o pożarze do systemu monitorowania PSP,
- ⇨ automatyczne uruchomienie wentylatorów wyciągowych oraz otwarcie klap instalacji wentylacji oddymiającej na korytarzach, w strefie pożarowej na kondygnacji, na której powstał pożar,
- ⇨ uruchomienie wentylatorów nawiewnych (nawiew i nadciśnienie w klatkach schodowych i do holi windowych, przepływ powietrza przez żaluzje do korytarzy na kondygnacji, na której powstał pożar);
- ⇨ automatyczne wyłączenie wentylatorów nawiewnych i wyciągowych wentylacji i klimatyzacji, obsługujących strefę, w której powstał pożar;
- ⇨ zamknięcie klap przeciwpożarowych na kanałach wentylacji ogólnej na kondygnacji, na której powstał pożar,
- ⇨ zatrzymanie dźwigów osobowych, sprowadzenie ich na parter budynku i pozostawienie z otwartymi drzwiami,
- ⇨ uruchomienie dźwiękowego systemu ostrzegawczego na kondygnacji, na której powstał pożar (komunikat ewakuacyjny) oraz sąsiadujących strefach pożarowych (komunikat informacyjny dla personelu),
- ⇨ zwolnienie kontroli dostępu oraz wysterowanie drzwi pożarowych i przesuwnych.

Działania podjęte przez pracowników ochrony i personel medyczny:

- ⇨ podjęcie działań gaśniczych podręcznym sprzętem gaśniczym i hydrantami – działanie ręczne,
- ⇨ po opanowaniu i likwidacji źródła pożaru: ponowne ustawienie centrali pożarowej na czuwanie,
- ⇨ ewakuacja pacjentów do strefy pożarowej na tej samej kondygnacji i klatką schodową na kondygnację niżej,
- ⇨ Wyłączenie dopływu gazów medycznych do strefy objętej pożarem po zakończeniu ewakuacji pacjentów z tej strefy.

Niezależnie od zadziałania systemu sygnalizacji pożaru i działań podjętych przez pracowników lub ochronę w przypadku rozwoju pożaru:

- ⇨ automatyczne uruchomienie urządzenia tryskaczowego.

Po przybyciu Straży Pożarnej :

- ⇨ przyjęcie działań gaśniczych przez Straż Pożarną,
- ⇨ wykonywanie poleceń wydawanych przez dowódcę Straży Pożarnej,

- ⇨ przekazanie komunikatów o ewakuacji w strefach pożarowych nie objętych pożarem za pomocą dźwiękowego systemu ostrzegawczego.

Algorytm dla pożaru powstałego w szybie windowym

Zasygnalizowanie na tablicy centrali pożarowej sygnału alarmu pożarowego.

Źródło informacji: czujka systemu sygnalizacji pożaru.

Automatyczne zadziałanie alarmu ograniczonego w centrali pożarowej – alarm I stopnia (czas trwania tego stanu jest ograniczony do 3 minut).

Sprawdzenie na miejscu źródła sygnału przez pracownika ochrony.

1. w przypadku drobnego incydentu: ręczna kasacja stanu alarmowanie i przestawienie centrali pożarowej na czuwanie,
2. w przypadku poważnego zagrożenia pożarowego - ręczne uruchomienie najbliżej położonego ROP – aktywacja alarmu II stopnia,
3. w przypadku braku reakcji po 3 minutach automatyczna aktywacja alarmu II stopnia.

Alarm II stopnia powoduje uruchomienie następującej sekwencji zdarzeń:

- ⇨ przekazanie sygnału o pożarze do systemu monitorowania PSP,
- ⇨ uruchomienie wentylatorów nawiewnych (nawiew i nadciśnienie w klatce schodowej oraz w przedsionku na 01);
- ⇨ zatrzymanie dźwigów osobowych, sprowadzenie ich na parter budynku i pozostawienie z otwartymi drzwiami,
- ⇨ uruchomienie dźwiękowego systemu ostrzegawczego w strefie holu windowego na 01.

Działania podjęte przez pracowników ochrony:

- ⇨ podjęcie działań gaśniczych podręcznym sprzętem gaśniczym i hydrantami – działanie ręczne,
- ⇨ po opanowaniu i likwidacji źródła pożaru: ponowne ustawienie centrali pożarowej na czuwanie.

Niezależnie od zadziałania systemu sygnalizacji pożaru i działań podjętych przez pracowników lub ochronę w przypadku rozwoju pożaru:

- ⇨ automatyczne uruchomienie urządzenia tryskaczowego.

Algorytm dla pożaru powstałego w pomieszczeniu technicznym

Z chwilą odebrania sygnału w centrali systemu sygnalizacji pożaru, opisane poniżej działania są wykonane automatycznie lub ręcznie przez pracowników ochrony.

Zasygnalizowanie na tablicy centrali pożarowej sygnału alarmu pożarowego.

Zadziałanie sygnalizatorów optycznych na kondygnacji, na której system wykrył pożar.

Źródło informacji: czujka systemu sygnalizacji pożaru.

Sprawdzenie na miejscu źródła sygnału przez pracownika ochrony.

1. w przypadku drobnego incydentu: ręczna kasacja stanu alarmowanie i przestawienie centrali pożarowej na czuwanie,
2. w przypadku poważnego zagrożenia pożarowego - ręczne uruchomienie najbliżej położonego ROP – aktywacja alarmu II stopnia,
3. w przypadku braku reakcji po 3 minutach automatyczna aktywacja alarmu II stopnia,

Alarm II stopnia powoduje uruchomienie następującej sekwencji zdarzeń:

- ⇨ przekazanie sygnału o pożarze do systemu monitorowania PSP,
- ⇨ automatyczne uruchomienie wentylatorów wyciągowych oraz otwarcie klap instalacji wentylacji oddymiającej na korytarzach, na kondygnacji na której powstał pożar,
- ⇨ uruchomienie wentylatorów nawiewnych (nawiew i nadciśnienie w klatkach schodowych i do holi windowych, przepływ powietrza przez żaluzje do korytarzy na kondygnacji, na której powstał pożar;
- ⇨ zatrzymanie dźwigów osobowych, sprowadzenie ich na parter budynku i pozostawienie z otwartymi drzwiami,
- ⇨ uruchomienie dźwiękowego systemu ostrzegawczego na kondygnacji , na której powstał pożar (komunikat ewakuacyjny) oraz sąsiadujących strefach pożarowych (komunikat informacyjny dla personelu).

Działania podjęte przez pracowników ochrony:

- ⇨ podjęcie działań gaśniczych podręcznym sprzętem gaśniczym i hydrantami – działanie ręczne,
- ⇨ po opanowaniu i likwidacji źródła pożaru: ponowne ustawienie centrali pożarowej na czuwanie.

Niezależnie od zadziałania systemu sygnalizacji pożaru i działań podjętych przez pracowników lub ochronę w przypadku rozwoju pożaru:

- ⇨ automatyczne uruchomienie urządzenia tryskaczowego.

Po przybyciu Straży Pożarnej :

- ⇨ przyjęcie działań gaśniczych przez Straż Pożarną,
- ⇨ wykonywanie poleceń wydawanych przez dowódcę Straży Pożarnej,
- ⇨ przekazanie komunikatów o ewakuacji w strefach pożarowych objętych pożarem za pomocą dźwiękowego systemu ostrzegawczego.

<u>Algorytm dla pożaru powstałego w pomieszczeniu dydaktycznym, biurowym, hotelowym, gospodarczym lub handlowym</u>

Z chwilą odebrania sygnału w centrali systemu sygnalizacji pożaru, opisane poniżej działania są wykonane automatycznie lub ręcznie przez pracowników ochrony.

Zasygnalizowanie na tablicy centrali pożarowej sygnału alarmu pożarowego.

Zadziałanie sygnalizatorów optycznych na kondygnacji, na której system wykrył pożar.

Źródło informacji: czujka systemu sygnalizacji pożaru.

Sprawdzenie na miejscu źródła sygnału przez pracownika ochrony.

1. w przypadku drobnego incydentu: ręczna kasacja stanu alarmowanie i przestawienie centrali pożarowej na czuwanie,
2. w przypadku poważnego zagrożenia pożarowego - ręczne uruchomienie najbliżej położonego ROP – aktywacja alarmu II stopnia,
3. w przypadku braku reakcji po 3 minutach automatyczna aktywacja alarmu II stopnia,

Alarm II stopnia powoduje uruchomienie następującej sekwencji zdarzeń :

- ⇨ przekazanie sygnału o pożarze do systemu monitorowania PSP,
- ⇨ automatyczne uruchomienie wentylatorów wyciągowych oraz otwarcie klap instalacji wentylacji oddymiającej na korytarzach, na kondygnacji, na której powstał pożar,
- ⇨ uruchomienie wentylatorów nawiewnych (nawiew i nadciśnienie w klatkach schodowych i do holi windowych, przepływ powietrza przez żaluzje do korytarzy na kondygnacji, na której powstał pożar;
- ⇨ zatrzymanie dźwigów osobowych, sprowadzenie ich na parter budynku i pozostawienie z otwartymi drzwiami,
- ⇨ uruchomienie dźwiękowego systemu ostrzegawczego na kondygnacji, na której powstał pożar (komunikat ewakuacyjny) oraz sąsiadujących strefach pożarowych (komunikat informacyjny dla personelu),
- ⇨ zwolnienie kontroli dostępu oraz wysterowanie drzwi pożarowych i przesuwnych.

Działania podjęte przez pracowników ochrony:

- ⇨ podjęcie działań gaśniczych podręcznym sprzętem gaśniczym i hydrantami – działanie ręczne,
- ⇨ po opanowaniu i likwidacji źródła pożaru: ponowne ustawienie centrali pożarowej na czuwanie.

Niezależnie od zadziałania systemu sygnalizacji pożaru i działań podjętych przez pracowników lub ochronę w przypadku rozwoju pożaru:

- ⇨ automatyczne uruchomienie urządzenia tryskaczowego.

Po przybyciu Straży Pożarnej :

- ⇨ przyjęcie działań gaśniczych przez Straż Pożarną,
- ⇨ wykonywanie poleceń wydawanych przez dowódcę Straży Pożarnej,
- ⇨ przekazanie komunikatów o ewakuacji w strefach pożarowych objętych pożarem za pomocą dźwiękowego systemu ostrzegawczego.

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.

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 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 nad sufitami podwieszonymi zastosowane projektuje czujki pożarowe wyposażone we wskaźniki zadziałania identyfikujące miejsce zainstalowania czujek z dokładnością do 1 m, jednocześnie jeden wskaźnik zadziałania może być dołączony do maksymalnie 4 czujek (pod warunkiem takiej funkcjonalności systemu) – zgodnie z wytycznymi SITP.

Początki i końce pętli dozorowych należy wykonać kablem HTKSHekw PH90. Pozostałą część pętli można wykonać kablem YnTKSYekw w powłoce koloru czerwonego (ze względu na brak wymogu dotyczącego ciągłości okablowania w warunkach pożaru). Należy zachować jednorodność średnicy żył kabli w pętlach. Wszędzie tam, gdzie kilka kabli jest prowadzonych obok siebie, okablowanie należy wykonać kablem HTKSHekw PH90. Długość i obciążalność pętli nie może przekroczyć dopuszczalnych parametrów granicznych określonych przez producenta systemu pożarowego. Należy stosować okablowanie zalecane przez producenta systemu.

Przewody pętli dozorowych należy prowadzić natynkowo pod przewodami niepalnymi, należy je mocować specjalnymi uchwytami ognioodpornymi, w odstępach co 30cm w odcinkach poziomych oraz co 45cm w odcinkach pionowych.

Przewody pętli sygnałowych, należy prowadzić w korytach kablowych – koryta ognioodporne E90, w przypadku braku koryt należy prowadzić je natynkowo mocować specjalnymi uchwytami ognioodpornymi, w odstępach co 30cm w odcinkach poziomych oraz co 45cm w odcinkach pionowych. W szachtach przewody należy prowadzić na drabinach kablowych.

Przewody pętli dozorowych i sygnałowych należy prowadzić z zachowaniem odpowiednich odległości od przewodów zasilających i opraw oświetleniowych. W żadnym wypadku nie prowadzić przewodów linii dozorowych lub sygnałowych SSP w jednym korycie instalacyjnym z przewodami instalacji elektrycznej. Przy przejściu przewodów do stref pożarowych należy zastosować odpowiednie uszczelnienia przepustów w celu utrzymania kryteriów szczelności i izolacyjności ogniowej.

Monitorowanie stanu oraz wysterowanie central systemu oddymiania będzie realizowane poprzez pętlowe moduły SSP. Moduły będą także monitorować stan zasilaczy pożarowych.

Monitorowanie stanu oraz wysterowanie instalacji tryskaczowej będzie realizowane poprzez pętlowe moduły SSP. Szczegółową lokalizację elementów pętlowych przewidzianych na potrzeby instalacji tryskaczowej należy skoordynować z projektem instalacji tryskaczowej na etapie realizacji inwestycji.

W celu umożliwienia połączenia pomiędzy centralami (projektowanymi i istniejącymi) projektuje się połączenia zgodnie z częścią rysunkową, w topologii pętli, tzn. pomiędzy centralami należy ułożyć dwa kable HTKSHekw 1x2x1.0, które w jak największym obszarze należy prowadzić osobnymi trasami.

Stan klap pożarowych musi być monitorowany przez SSP. Zamkniecie jakiejkolwiek klapy pożarowej uniemożliwi uruchomienie centrali wentylacyjnej w obwodzie której znajdowała się dana klapa. 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 nie naruszający. 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.

Po integracji z istniejącym systemem należy go ponownie zaprogramować zachowując dotychczasowe scenariusze pożarowe i algorytmy sterowań, ale z uwzględnieniem sygnałów przesyłanych z projektowanego systemu.

<u>Zintegrowany system zarządzania bezpieczeństwem pożarowym - wymagania</u>

Zintegrowany system zarządzania bezpieczeństwem pożarowym musi umożliwiać sterowanie urządzeniami przeciwpożarowymi oraz wdrożenie procedur ułatwiających nadzór nad bezpieczeństwem obiektu. System będzie posiadał procedury i instrukcje ułatwiające obsługę codzienną systemu sygnalizacji pożarowej, sterowania urządzeniami ppoż., oraz systemów powiązanych – w tym przetwarzanie alarmu pożarowego i możliwość ręcznego nadrzędnego sterowania przy wykorzystaniu stacji operatorskiej. System zapewni

sterowanie klapami na wentylacji pożarowej a w przypadku pożaru przesterowanie wentylacji w celu ograniczenia skutków pożaru i usprawnienia ewakuacji ludzi (pacjentów /personelu /gości) z obiektu.

Interfejs systemu będzie bazował na grafice wektorowej i na elastycznej platformie programowej umożliwiającej dostosowanie do indywidualnych wymagań użytkownika. Współpraca systemu zarządzania bezpieczeństwem pożarowym z systemami bezpieczeństwa i zakres integracji musi być dostosowany do funkcjonalności wymaganych dla zapewnienia bezpieczeństwa pożarowego oraz sprawnej ewakuacji ludzi z budynku.

Zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji, do sterowania urządzeniami przeciwpożarowymi muszą być stosowane certyfikowane centrale sterujące – projektowany w obiekcie zintegrowany system zarządzania bezpieczeństwem pożarowym musi posiadać świadectwo dopuszczenia CNBOP do sterowania urządzeniami ppoż.

Serwer systemu zarządzania bezpieczeństwem pożarowym musi być instalowany w szafie RACK, być serwerem redundantnym opartym na jednostkach o zwiększonej niezawodności oraz posiadać redundantne zasilanie buforowe i układ przełączający w przypadku awarii jednostki głównej serwera. Komunikacja serwera z siecią central sygnalizacji pożarowej, sterowania urządzeniami pożarowymi i sterowania urządzeniami gaśniczymi musi być oparta o łącze redundantne.

Stacje operatorskie systemu zarządzania bezpieczeństwem pożarowym - komunikacja pomiędzy stacją operatorską a serwerem systemu będzie ciągle monitorowana. Stacja operatorska musi być wyposażona w trzy monitory Full HD o przekątnej ekranu min. 24 cale.

Elementy wykonawcze (polowe) systemu zarządzania bezpieczeństwem pożarowym wykorzystywane między innymi do sterowania i nadzorowania klap przeciwpożarowych zostaną w pełni zintegrowane z systemem sygnalizacji pożarowej bądź będą bazowały na niezależnych sterownikach bądź centralach sterowania urządzeniami ppoż. Elementy wykonawcze dla klap na wentylacji pożarowej muszą nadzorować ciągłość linii sterująco-zasilającej siłownika klapy oraz posiadać funkcję fail-safe umożliwiającą wysterowanie przekaźnika w pozycję pożarowo-bezpieczną w przypadku zaniku komunikacji elementu z centralą/sterownikiem/serwerem systemu.

Zakres realizowanych funkcji/procedur przez zintegrowany system zarządzania bezpieczeństwem ppoż.:

- Wizualizacja na planach graficznych wszystkich nadzorowanych systemów – elementy w warstwach technicznych.
- Obsługa elementów systemów bezpieczeństwa pożarowego
  - odłączanie, załączanie, wysterowanie, kasowanie
  - dostęp do dokumentacji technicznej powiązanej z wizualizowanymi urządzeniami przeciwpożarowymi
  - sygnalizacja stanów niebezpiecznych i krytycznych w systemie bezpieczeństwa pożarowego
  - sygnalizacja stanów uszkodzenia
  - przeglądanie elementów na warstwach technicznych
- Procedura obsługi alarmu pożarowego (1 stopień / 2 stopień)
  - alarm 1 stopnia / alarm 2 stopnia

  - weryfikacja/potwierdzenie alarmu z uwzględnieniem systemu nadzoru wizyjnego
  - sterowanie funkcją alarmowania 2-stopniowego - opóźnienie aktywne/nieaktywne
  - przyjmowanie zdarzenia przez operatora oraz opis przyczyny alarmu
  - instrukcja postępowania dla operatora
- Procedury ręcznych/nadrzędnych sterowań urządzeniami ppoż oraz urządzeniami/systemami technicznymi i bezpieczeństwa
- Procedura obsługi uszkodzeń/stanów niewłaściwych
  - przyjmowanie zdarzenia przez obsługę
  - obsługa uszkodzenia
  - - opis zdarzenia,
  - - wezwanie serwisu,
  - - komentarze operatora
  - dodawanie i opisywanie zdarzeń zewnętrznych
  - raportowanie
- Procedura obsługi dwustopniowej wyjść krytycznych w systemie sygnalizacji pożarowej
  - Potwierdzanie wykonywanych sterowań - funkcja bezpieczeństwa
- Rejestracja wszystkich zdarzeń, analiza danych historycznych i generowanie raportów systemowych

<u>Zintegrowany system zarządzania bezpieczeństwem pożarowym – opis systemu i charakterystyka ogólna projektowanego systemu SIS-FIRE</u>

W obiekcie przewiduje się zastosowanie zintegrowanego systemu zarządzania bezpieczeństwem pożarowym SIS-FIRE, który wykorzystywany będzie do wizualizacji, sterowania i zarządzania urządzeniami przeciwpożarowymi z wykorzystaniem innych systemów bezpieczeństwa w obiekcie takich jak system sygnalizacji pożarowej. System zapewnia maksymalny poziom ochrony poprzez utworzenie jednego, spójnego, w pełni kompatybilnego i kompleksowego narzędzia nadzoru nad bezpieczeństwem pożarowym budynku.

Istotną cechą systemu zarządzania bezpieczeństwem pożarowym SIS-FIRE jest jego wysoka elastyczność działania i możliwość spełnienia niemal nieograniczonej liczby zadań i funkcji logicznych. Elementy integratora są dowolnie programowalne i realizują funkcje bezpieczeństwa zgodnie z przyjętymi założeniami i scenariuszem pożarowym zabezpieczanego obiektu, współpracując przy tym bezpośrednio (certyfikowane połączenie cyfrowe) z systemem sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi.

Konfiguracja i zakres funkcji integracji (sterowanie, nadzorowanie, zarządzanie) w systemie SIS-FIRE mogą być programowane oddzielnie dla każdego z elementów składowych systemu takich jak serwer systemu wraz z platformą informatyczną i centrale sterowania urządzeniami ppoż. Funkcje systemu mogą być dostosowywane do indywidualnych, bardzo rozbudowanych wymagań bezpieczeństwa pożarowego dla każdego rodzaju obiektu. Każdy z elementów integratora może jednocześnie realizować swoje funkcje niezależnie od pozostałych podzespołów systemu, eliminując całkowicie ryzyko awarii totalnej, nawet w przypadku wielopunktowych uszkodzeń linii nadzorujących, torów komunikacji, całkowitego zaniku lub chwilowej awarii zasilania.

SIS-FIRE zgodnie z certyfikatem oraz świadectwem dopuszczenia CNBOP, do sterowania urządzeniami ppoż. może wykorzystywać centrale sygnalizacji pożarowej/sterowania urządzeniami ppoż. INTEGRAL IP wraz z modułami we/wy techniki X-LINE.

SIS-FIRE jako centrala sterująca urządzeniami przeciwpożarowymi posiada certyfikat oraz świadectwo dopuszczenia CNBOP uwzględniające możliwość sterowania urządzeniami przeciwpożarowymi.

Zintegrowany system zarządzania bezpieczeństwem pożarowym (system integrujący urządzenia ppoż) SIS-FIRE w obiekcie składa się z następujących komponentów:

- centrale sygnalizacji pożarowej / sterowania urządzeniami przeciwpożarowymi INTEGRAL IP
  - 42 centrale INTEGRAL IP pracujące w sieci (część istniejąca i projektowana)– detekcja i sterowanie urządzeń ppoż
  - 1 centrala główna INTEGRAL IP – zarządzanie systemem sieciowym złożonym z sześć niezależnych podsystemów (system detekcji i sterowania urządzeń ppoż, sterowanie stałymi urządzeniami gaśniczymi).
  - moduły sterujące wejścia/wyjścia do sterowania i nadzorowania urządzeń przeciwpożarowych
- platforma informatyczna systemu integrującego SIS-FIRE
  - stanowisko redundantnego serwera w szafie RACK, redundantne zasilanie z zasilaczy buforowych z podtrzymaniem awaryjnym, jednostki komputerowe o zwiększonej niezawodności. Oprogramowanie systemowe z wymaganymi licencjami i interfejsami do integrowanych systemów bezpieczeństwa w obiekcie (ssp, dso, sys. przyzywowy)
  - trzy stacje operatorskie (klient)

<u>Wytyczne dla inwestora, użytkownika i wykonawcy</u>

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.

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 czujek, stref i linii,
- dokumentację techniczną (powykonawczą) systemu zawierającą opis jego działania, sposób zasilania, umożliwiającą łatwą identyfikację linii dozorowych, stref, nadzorowanych pomieszczeń, rodzajów czujek i innych elementów 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 oraz scenariusza pożarowego sporządzi szczegółową matrycę sterowań i

scenariusz rozwoju zdarzeń w czasie pożaru. Dokument ten powinien stanowić załącznik do instrukcji bezpieczeństwa pożarowego z planem ewakuacji i powinien zostać zaakceptowany przez Projektanta Projektu Budowlanego oraz uzgodniony przez rzeczoznawcę ds. zabezpieczeń przeciwpożarowych uzgadniającego Projekt Budowlany.

W związku z tym, że projekt przewiduje instalację central SSP w wydzielonych pomieszczeniach teletechnicznych bez stałego nadzoru należy przewidzieć instalację dodatkowych wyniesionych paneli w pomieszczeniach ochrony, w których przewiduje się całodobowy dozór wykwalifikowanego personelu.

W wybranych pomieszczeniach (salach operacyjnych, poznieczuleniowych, IT i WC niepełnosprawnych oraz wentylatorniach sanitarnych należy zainstalować dodatkowe sygnalizatory optyczne.

Czujniki zainstalowane w przestrzeniach zamkniętych międzystropowych należy wyposażyć w zewnętrzne wskaźniki zadziałania, identyfikujące miejsce zainstalowania czujek z dokładnością do 1,0 m.

Na etapie realizacji instalacji należy ostatecznie skoordynować lokalizację poszczególnych elementów systemu sygnalizacji pożarowej zgodnie z wytycznymi dotyczącymi zasad montażu tych elementów. W szczególności dotyczy to lokalizacji czujek pożarowych względem urządzeń wentylacyjnych, elektrycznych i elementów architektonicznych (np. podciągi) oraz lokalizacji wskaźników zadziałania. W związku z możliwością wystąpienia na etapie realizacji nieujętych w niniejszej dokumentacji elementów (np. podciągi) w przedmiarze przewidziano odpowiednią rezerwę urządzeń SSP

5.2 Instalacja oddymiania pożarowego i napowietrzania w budynku A1

Szczegóły rozwiązań wg branży sanitarnej.

W budynku A1 projektuje się pętlowe modułu sterujące, które przewiduje się do sterowania i monitorowania wszystkich klap i urządzeń pożarowych, których praca musi być zagwarantowana w trakcie pożaru: baterie klap (oddymiających i napowietrzających, klapy odcinające wentylatorów nawiewnych, klapy systemu nadciśnienia, brama pożarowa itp.)

Proces zapobiegania zadymieniu będzie uruchamiany sygnałem z centrali SSP za pomocą styków bezpotencjałowych, po wykryciu przez SSP pożaru w danej strefie pożarowej. Po otrzymaniu sygnału o rozpoczęciu procesu oddymiania zostaną wysterowane siłowniki klap oddymiających oraz wentylatory napowietrzające. Główne elementy systemu oddymiania będą monitorowane w SSP, w tym stan klap pożarowych na kanałach. Każde uruchomienie procesu oddymiania i napowietrzania, a także awaria systemu zostanie zarejestrowana w pamięci centrali pożarowej.

W ramach realizacji zadania w budynku A1 (wykonanie kompletnych instalacji na poziomach P00 i P3) należy wykonać także w ograniczonej części instalacje niezbędne do realizacji celu jakim jest prawidłowe funkcjonowanie instalacji oddymiania pożarowego zgodnie z planem realizacji CKD2.

W związku z powyższym należy wykonać sterowanie następujących urządzeń:

- sterowanie wentylatora nawiewnego klatki KL1 – PNKL-1

- sterowanie czujników statycznej różnicy ciśnień w klatce KL1 (5 szt.)

- sterowanie i monitorowanie klap pożarowych w zakresie niezbędnym do realizacji CKD2 (kondygnacje techniczne, klatki schodowe, pomieszczenia techniczne i ciągi komunikacyjne

na drogach do tych pomieszczeń zgodnie z Planem Realizacji CKD2). Szczegółowy wykaz klap pożarowych, przepustnic i innych urządzeń zapobiegających zadymieniu wymagających sterowania zawarty jest w projekcie branży sanitarnej.

5.3 Instalacja oddymiania grawitacyjnego budynku A2

Opis systemu

Na potrzeby oddymiania klatek schodowych budynku A2 projektuje się instalację systemu oddymiania grawitacyjnego powiązanego z Systemem Sygnalizacji Pożaru. Projektowana instalacja oddymiania ma na celu zapewnić sprawną ewakuację w czasie zagrożenia pożarem poprzez usunięcie dymu z klatek schodowych na zewnątrz budynku poprzez automatycznie otwierane klapy dymowe oraz równolegle otworzenie otworów napowietrzających na parterze.

Sterowanie (uruchomienie po wykryciu pożaru) oddymiania następuje w momencie detekcji zagrożenia pożarowego przez czujki dymu zainstalowane na klatkach schodowych, monitorowanie stanu central oddymiania (praca/awaria) będzie odbywać się za pomocą pętlowych modułów kontrolno-sterujących SSP z wykorzystaniem styków bezpotencjałowych.

Detekcja zagrożenia pożarowego będzie realizowana za pomocą czujek dymu podłączonych bezpośrednio do central oddymiania. Projektuje się zainstalowanie dwóch central (CSO), po jednej na każdą klatką schodową. Centrale należy zamontować na ostatnich kondygnacjach w pobliżu klap dymowych. Powinny być zamontowane w pobliżu stropu, w sposób zapewniający widoczność diod sygnalizacyjnych na każdej z central. Każda z central powinna być wyposażona w co najmniej dwa moduły: jeden dedykowany na potrzeby sterowania siłownikami otworów napowietrzających a drugi na potrzeby klapy dymowej.

Na ostatniej kondygnacji każdej z klatek schodowych projektuje się zainstalowanie klapy dymowej o minimalnej powierzchni czynnej nie mniej niż 5% rzutu poziomego klatki. Szczegóły obliczeń powierzchni czynnych klap oraz otworów napowietrzających wg projektu branży architektonicznej.

Przy centralach CSO oraz na parterze każdej klatki schodowej należy zainstalować awaryjne przyciski oddymiania. Należy stosować przyciski dedykowane dla systemów oddymiania. Przy awaryjnych przyciskach oddymiania należy również zainstalować przyciski przewietrzania.

W celu zabezpieczenia klap oddymiających przed silnym wiatrem oraz klatek schodowych przez zalaniem wodą na wypadek pożaru należy zainstalować czujniki pogodowe, które automatycznie zamkną klapy na wypadek opadów lub silnego wiatru. W przypadku wystąpienia alarmu pożarowego klapy otworzą się bez względu na warunki pogodowe. Graniczna wartość opadów oraz siły wiatru powinna być regulowana.

System będzie zapewniał możliwość oddymiania klatek schodowych na wypadek alarmu oraz przewietrzania w czasie normalnej eksploatacji obiektu.

W przypadku alarmu drzwi zlokalizowane na parterze klatek schodowych mają otworzyć się automatycznie. W celu uniknięcia zakleszczenia drzwi należy wprowadzić zwłokę pomiędzy rozpoczęciem automatycznego otwierania skrzydła czynnego oraz biernego drzwi. Drzwi należy wyposażyć w siłowniki kompatybilne z zaprojektowaną centralą.

Dostawa klap dymowych z siłownikami oraz drzwi napowietrzających wraz z siłownikami w zakresie branży architektonicznej.

Zasilanie

Każdą z centralek oddymiania należy wyposażyć w zasilacz buforowy umożliwiający bezawaryjną pracę instalacji oddymiania przez 72h po zaniku zasilania głównego. Po tym czasie możliwe będzie minimum jednokrotne alarmowe zadziałanie systemu. Centralki będą zasilane napięciem 230V AC, kablem PH90 sprzed głównego wyłącznika prądu z głównej rozdzielnicy pożarowej budynku.

Okablowanie

Podłączenie siłowników klap oddymiających oraz napędów drzwi należy wykonać przewodami HLGs 2x2,5 mm2 PH90 lub równoważnymi. Przyciski alarmowego oddymiania należy podłączyć do central wykorzystując przewód HTKSH 4x2x0,8. Połączenie central pogodowych oraz przycisków przewietrzania należy wykonać przewodem YTKSY lub YDY.

Do instalacji bezpieczeństwa pożarowego należy stosować przewody odpowiedniego typu posiadające wymagane przepisami dopuszczenia i certyfikaty. Sposób prowadzenia i mocowania przewodów do podłoża powinien być zgodny z wymaganiami w zakresie ochrony przeciwpożarowej i wytycznymi producenta przewodu. Puszki rozgałęźne i przyłączeniowe do przewodów o odporności ogniowej powinny posiadać klasę PH i dopuszczenia zgodnie z obowiązującymi przepisami i wymaganiami stawianymi instalacjom w obiekcie. Przejścia przez przegrody i ściany rozdzielające strefy pożarowe należy uszczelnić do wymaganej klasy odporności ogniowej. Okablowanie wykonać zgodnie z zaleceniami producenta. System należy zabezpieczyć przeciwprzepięciowo.

Wytyczne dla inwestora, użytkownika i wykonawcy

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,
- dokumentację techniczną (powykonawczą) systemu zawierającą opis jego działania, sposób zasilania, umożliwiającą łatwą identyfikację zainstalowanych urządzeń.

W czasie odbioru Wykonawca systemu oddymiania 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 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.

5.4 Dźwiękowy System Ostrzegawczy

Zakres realizacji

Na potrzeby budynków A1 oraz A2 projektuje się Dźwiękowy System Ostrzegawczy. Dla budynku A1 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), natomiast dla budynku A2 projektuje się jego zastosowanie jako uzupełnienie ochrony przeciwpożarowej.

Zasięgiem systemu DSO objęty będzie 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.

Opis systemu

System będzie kompatybilny z istniejącym w kompleksie szpitalnym DSO. Po dołączeniu nowych elementów DSO należy przeprogramować, uwzględniając nowe szafy oraz strefy nagłośnieniowe.

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

Szafy sterujące systemu będą instalowane w wydzielonym pożarowo pomieszczeniu technicznym. Dopuszcza się wykorzystanie rozproszonej lokalizacji szaf pod warunkiem, ze system posiada stosowne certyfikaty i dopuszczenia na taką funkcjonalność. 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 w przenoszonym pomieszczeniu monitoringu w budynku A1. W tym pomieszczeniu znajduje się mikrofon strażaka do prowadzenia akcji ewakuacyjnej. W budynku A2 natomiast przewiduje się zlokalizować mikrofon strażaka w pomieszczeniu monitoringu. Przy każdej z szaf zaprojektowano także mikrofony strażaka.

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 - 75dB

Dla budynku A2 przyjęto podział na 24 odrębne stref alarmowe. 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.

W zakresie niniejszego opracowania jest wykonanie kompletnej instalacji DSO na poziomy P00 i P3 oraz częściowo na pozostałych poziomach w zakresie niezbędnym do prawidłowego i zgodnego z przepisami funkcjonowania wszystkich instalacji będących w zakresie zamierzenia realizacyjnego

Dla budynku A1 przyjęto podział na 43 odrębne strefy alarmowe. 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 dwóch linii głośnikowych.

Elementy sterujące systemu i wzmacniacze zainstalowane będą w szafach RACK 19". Jednostka centralna DSO znajdować się będzie w szafach przystosowanych i certyfikowanych dla systemu DSO. Szafy wyposażone będą 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.

Linie głośnikowe należy prowadzić od głośnika do głośnika, przy wejściu przewodu do głośnika należy zastosować dławnicę certyfikowaną. Przewody należy układać z zachowaniem siły wciągania i promienie gięcia zgodnie z wytycznymi producenta okablowania. Głośniki należy zakotwić, np. przy pomocy linki stalowej, do stałego elementu budynku, np. stropu. Główne ciągi kablowe należy prowadzić z wykorzystaniem zaprojektowanych tras i uchwytów pożarowych, natomiast odejścia mocować bezpośrednio do stropu na metalowych uchwytach (co 30cm). Mocowanie do podłoża przy pomocy atestowanych uchwytów stalowych i kołków rozporowych stalowych. Przewód nie może podlegać obciążeniom mechanicznym, także w czasie pożaru i nie będzie łączony w innych miejscach jak głośniki (wyposażone w kostki podłączeniowe ceramiczne oraz w zabezpieczenia termiczne). Zespoły kablowe powinny

posiadać certyfikat potwierdzający ich właściwości pożarowe odnoszący się do zespołu jako zestawu określonych wyrobów (konkretny kabel wraz z konkretnym mocowaniem).

Instalacja okablowania musi być wykonana z uwzględnieniem elementów budowlanych oraz instalacji branżowych ciągów wentylacyjnych, instalacji rurowych i elektrycznej.

Wszystkie przejścia przewodów przez przegrody pomiędzy strefami pożarowymi należy bezwzględnie uszczelnić masą plastyczną o odporności ogniowej odpowiadającej odporności ścian lub stropów, przez które wykonano te przejścia (posiadające odpowiednie i aktualne certyfikaty) np. ochronną masą uszczelniającą HILTI lub PROMAT.

Łączenie czy sztukowanie (lutowanie, skręcanie, puszki łączeniowe niecertyfikowane) linii głośnikowej jest niedopuszczalne.

W projekcie przewidziano mikrofony strażaka, które będą umożliwiać wybór strefy rozgłaszania oraz nadawania komunikatów na wypadek zagrożeń pożarowych oraz innych mogących wpłynąć na bezpieczeństwo osób przebywających w obiekcie. Słowne komunikaty nadawane z mikrofonu strażaka w trybie alarmowym będą posiadały najwyższy priorytet. Oznacza to, iż podczas ich nadawania będą wstrzymywane komunikaty automatyczne w danej strefie. 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.

Przyjęto poniższe założenia dla systemu:

- Pewność działania – przyjęto, że w przypadku awarii linii głośnikowej przynajmniej połowa głośników w danej strefie pożarowej będzie sprawna.
- Konfiguracja linii głośnikowych – przyjęto typ A/B, w którym dwie konwencjonalne promieniowe linie głośnikowe nagłaśniają tą samą przestrzeń. Przerwa lub zwarcie w jakiejkolwiek linii są wykrywane jako uszkodzenie.
- Słyszalność dźwięku alarmu powyżej szumu tła (stosunek odstępu sygnału od szumu) od 6dB do 20dB
- Zrozumiałość mowy w obszarze pokrycia powinna być większa albo równa 0,7 CIS (0,5 STI).
- Dla obiektu przyjęto podział na odrębne strefy alarmowe, które zostały wydzielone zgodnie z podziałem na strefy pożarowe.
- W każdej strefie pożarowej 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.
- Szafy centrali DSO zlokalizowane w jednym pomieszczeniu. Dopuszcza się możliwość lokalizacji rozproszonej pod warunkiem posiadania przez zastosowany system stosownych certyfikatów i świadectw.

Właściwości systemu

Węzły sieci wyposażone są odpowiednio w:

Szafa DSO1-A2/1 - Szafa 600x600, 42U z zestawem baterii akumulatorów i zasilaczem:

- 1x interfejs wielokanałowy
- 4x wzmacniacz roboczy 4x125W
- 1x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- 1x rozdzielacz sieciowy sygnały
- Mikrofon strażaka + klawiatury rozszerzeń

Szafa DSO2-A2/2 - Szafa 600x600, 42U z zestawem baterii akumulatorów i zasilaczem:

- 1x interfejs wielokanałowy
- 3x wzmacniacz roboczy 4x125W
- 1x wzmacniacz roboczy 2x250W
- 1x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- Mikrofon strażaka + klawiatury rozszerzeń

Szafa DSO3-A2/3 - Szafa 600x600, 42U z zestawem baterii akumulatorów i zasilaczem:

- 1x interfejs wielokanałowy
- 2x wzmacniacz roboczy 4x125W
- 2x wzmacniacz roboczy 2x250W

- 1x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- Mikrofon strażaka + klawiatury rozszerzeń

Szafa DSO4-A2/4 - Szafa 600x600, 42U z zestawem baterii akumulatorów i zasilaczem:

- 2x interfejs wielokanałowy
- 2x wzmacniacz roboczy 4x125W
- 2x wzmacniacz roboczy 2x250W
- 1x wzmacniacz roboczy 1x60W
- 2x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- Mikrofon strażaka + klawiatury rozszerzeń

Szafa DSO1-A1/1 - Szafa 600x800, 42U z zestawem baterii akumulatorów i zasilaczem:

- 2x interfejs wielokanałowy
- 2x wzmacniacz roboczy 2x250W
- 3x wzmacniacz roboczy 4x125W
- 1x wzmacniacz roboczy 8x60W
- 2x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- Mikrofon strażaka + klawiatura rozszerzeń

Szafa DSO2-A1/2 - Szafa 600x800, 42U z zestawem baterii akumulatorów i zasilaczem:

- 1x interfejs wielokanałowy
- 2x wzmacniacz roboczy 4x125W
- 1x wzmacniacz roboczy 1x60W
- 1x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- Mikrofon strażaka + klawiatury rozszerzeń

Szafa DSO3-A1/3 - Szafa 600x800, 42U z zestawem baterii akumulatorów i zasilaczem:

- 1x interfejs wielokanałowy
- 1x wzmacniacz roboczy 4x125W
- 1x wzmacniacz roboczy 2x250W
- 1x wzmacniacz roboczy 1x60W
- 1x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- Mikrofon strażaka + klawiatury rozszerzeń

Szafa DSO4-A1/4 - Szafa 600x800, 42U z zestawem baterii akumulatorów i zasilaczem:

- 1x interfejs wielokanałowy
- 2x wzmacniacz roboczy 4x125W
- 2x wzmacniacz roboczy 2x250W
- 1x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- Mikrofon strażaka + klawiatury rozszerzeń

Szafa DSO5-A1/5 - Szafa 600x800, 42U z zestawem baterii akumulatorów i zasilaczem:

- 2x interfejs wielokanałowy
- 1x wzmacniacz roboczy 2x250W
- 2x wzmacniacz roboczy 4x125W
- 2x wzmacniacz roboczy 8x60W
- 2x wzmacniacz rezerwowy 1x500W
- 2x interfejs światłowodowy
- Mikrofon strażaka + klawiatura rozszerzeń

Schemat połączeń centrali DSO - na rysunkach projektowych.

Umieszczenie szaf wg rysunków projektowych. Ostateczne miejsce umieszczenia szaf, należy skorygować na etapie budowy.

Opis systemu

System umożliwia cyfrowe przetwarzanie sygnału audio oraz transmisję tego sygnału za pośrednictwem prostego systemu sieciowego. Transport sygnałów audio odbywa się całkowicie w formie cyfrowej poza ostatnim odcinkiem linii głośnikowej 100 V, począwszy od wzmacniacza mocy. Istnieje możliwość funkcjonowania systemu z dołączonym lub bez dołączonego komputera PC do sterownika sieciowego. Sterownik sieciowy wykorzystuje technologię sieciową (sieci informatyczne).

Dźwiękowy system ostrzegawczy stanowi sieciowy system zarządzania dźwiękiem. Poszczególne elementy systemu łączone są w konfiguracji łańcuchowej. Połączenia międzymodułowe wykonuje się za pomocą plastikowych lub szklanych kabli światłowodowych. Poszczególne moduły posiadają indywidualne adresy, które są automatycznie identyfikowane przez sterownik sieciowy. Poszczególne adresy wprowadza użytkownik, a sterownik sieciowy weryfikuje te dane. Sterownik sieciowy jest wyposażony w interfejs sieci Ethernet i RS-232. Okablowanie systemowe powinno zostać tak skonfigurowane, aby pojedyncza awaria w systemie nie przerywała pracy całego systemu.

Kabel światłowodowy służy do przesyłania zarówno systemowych sygnałów sterujących jak i sygnałów audio. Każde urządzenie systemowe spełniające rolę wejścia lub wyjścia jest wyposażone w odpowiednie funkcje przetwarzania sygnału audio. Proces przetwarzania odbywa się w dziedzinie cyfrowej. Przyjazny dla użytkownika interfejs obsługi umożliwia łatwe dokonywanie odpowiednich nastaw procesora dźwięku w zależności od rodzaju sygnałów na wejściu i wyjściu.

Rodzina urządzeń wchodzących w skład systemu nagłośnieniowego i dźwiękowego systemu ostrzegawczego składa się ze sterowników sieciowych, interfejsów wielokanałowych, wzmacniaczy mocy, stacji wywoławczych, ekspanderów audio oraz wysoko- i niskopoziomowych interfejsów systemów zewnętrznych. Poprawność działania wszystkich elementów systemu jest stale nadzorowana. Wszelkie nieprawidłowości są zgłaszane do sterownika sieciowego. Każdy wejściowy lub wyjściowy moduł audio jest wyposażony w gniazdo słuchawkowe umożliwiające monitorowanie sygnałów fonicznych. Sterownik sieciowy jest również wyposażony w głośnik umożliwiający monitorowanie sygnałów audio.

System nagłośnieniowy może spełniać szereg funkcji. Poniżej wymieniono najważniejsze z nich:

- System nagłośnieniowy stanowi medium do przekazywania do publicznej wiadomości instrukcji postępowania w nagłych przypadkach i do emisji komunikatów alarmowych.
- System nagłośnieniowy umożliwia emisję różnych komunikatów w różnych częściach obsługiwanego obiektu.
- System nagłośnieniowy stanowi medium do emisji tła muzycznego we wszystkich lub wybranych częściach obsługiwanego obiektu.
- System nagłośnieniowy umożliwia automatyczną emisję instrukcji postępowania w nagłych przypadkach i emisję komunikatów alarmowych.
- System przechowuje w pamięci sterownika sieciowego co najmniej 200 ostatnich komunikatów o błędach systemowych. Wszelkie zmiany w systemie mogą być odnotowywane we współpracującym komputerze PC. Dołącza się go do sterownika sieciowego za pośrednictwem karty sieci Ethernet.

W poniższych punktach zawarto zadania, jakie może realizować system w konfiguracji maksymalnej.

- Kierowanie sygnałów audio z dowolnego wejścia na dowolne wyjście. Połączenia są całkowicie programowalne.
- Kierowanie sygnałów tła muzycznego z wielu źródeł do różnych stref nagłośnieniowych lub wyjść audio.
- Komunikacja za pośrednictwem min. 28 kanałów audio (równoległa transmisja 28 sygnałów audio w tym samym czasie).
- Możliwość programowania funkcji systemowych za pośrednictwem dostarczonego oprogramowania konfiguracyjnego.
- Możliwość dołączenia sterownika sieciowego do lokalnej sieci budynku. Autoryzowany dostęp do sterownika za pośrednictwem sieci jest możliwy z dowolnej stacji roboczej dołączonej do sieci. Dostęp jest zabezpieczony hasłem.
- Sterowanie transmisją wywołań i realizacją innych funkcji w oparciu o nastawy systemu priorytetowego.
- Monitorowanie poprawności działania systemowych wzmacniaczy mocy i w razie awarii automatyczne przełączanie dodatkowych wzmacniaczy rezerwowych.
- Wykrywanie uszkodzeń w systemowych liniach głośnikowych związanych z wzajemnym zwarciem żył, rozłączeniem i zwarciem do ziemi. Linia głośnikowa jest medium wykorzystywanym wyłącznie do przesyłania sygnałów audio między głośnikami a wzmacniaczami mocy.
- Możliwość włączania w tory sygnałowe wejść i wyjść audio cyfrowych, parametrycznych korektorów charakterystyki przenoszenia.
- Przekaz sygnałów audio między wszystkimi modułami systemowymi w formie cyfrowej.
- System wyposażony jest w interfejsy umożliwiające dołączanie systemów zewnętrznych za pośrednictwem specjalnych złączy lub wyjść sterujących. Interfejsy umożliwiają wymianę informacji o awariach systemu i wszelkich zmianach w jego konfiguracji.
- Możliwość łatwej rozbudowy systemu przez dołączanie nowych modułów sprzętowych i uaktualnienie konfiguracji programowej.
- Bardzo ergonomiczne systemowe stacje wywoławcze. Ich wyposażenie umożliwia operatorowi zorientowanie się, czy w danej chwili wybrane wyjścia są zajęte przez wywołania o niższym lub wyższym priorytecie. Dzięki wbudowanemu głośnikowi

operator ma również możliwość odsłuchu sygnału gongu poprzedzającego wywołanie lub komunikatu cyfrowego.
- Możliwość monitorowania poprawności działania każdego elementu składowego systemu począwszy od kapsuły mikrofonu, a skończywszy na linii głośnikowej. Sygnał o każdej awarii jest wysyłany do sterownika sieciowego.
- Kanały końcowych wzmacniaczy mocy typu PAM są wyposażone w cyfrowe linie opóźniające. Wartość opóźnienia jest ustawiana za pośrednictwem oprogramowania konfiguracyjnego.

Specyfikacja funkcjonalna

- System powinien zostać tak zaprojektowany, aby istniała możliwość indywidualnego wyboru każdej strefy nagłośnieniowej / ostrzegawczej (alarmowej) / funkcjonalnej.
- Cały obiekt powinien zostać podzielony w szereg stref alarmowych. Każda ze stref alarmowych powinna zawierać jedną lub kilka stref nagłośnieniowych. System powinien zostać tak zaprojektowany, aby istniała możliwość indywidualnego wyboru każdej strefy alarmowej.
- W każdym miejscu okablowania systemowego istnieje możliwość doprowadzenia zasilania do systemu. Może to być zrealizowane za pośrednictwem rozgałęźnika sieciowego lub interfejsu światłowodowego.
- Sterownik sieciowy, wzmacniacze mocy PAM oraz moduł ekspandera audio są wyposażone w wyświetlacze LCD z 2 liniami po 16 znaków, które służą do wyświetlania informacji o aktualnych nastawach urządzenia.
- System stale monitoruje poprawność działania każdego z modułów systemowych i okablowania. Nieprawidłowości wszelkiego rodzaju są zgłaszane do sterownika sieciowego.
- System może być konfigurowany za pośrednictwem komputera PC dołączonego do sterownika sieciowego. Możliwa jest również samodzielna praca sterownika sieciowego.
- System może emitować komunikaty alarmowe (wywołania do wszystkich stref – all calls) nawet wtedy, gdy uszkodzeniu ulegnie sterownik sieciowy.
- Każdy element systemowy może zostać logicznie wyłączony z systemu, nawet jeśli fizycznie dalej będzie do niego dołączony.
- System może włączać lub wyłączać każde wejście i wyjście systemowe.
- Sterownikowi sieciowemu powinien być przypisany adres IP z dowolnego zakresu.
- Wzmacniacze mocy wyposażone są w wyłączniki zasilania umieszczone na płycie tylnej. Uniemożliwia to przypadkowe ich wyłączenie.
- Poszczególnym strefom nagłośnieniowym można przypisać trzy presety głośności emitowanych sygnałów zaprogramowanych o określonych godzinach. Dwa presety dostępne są dla muzyki w tle, jeden preset przeznaczony jest dla wywołań.
- Wentylatory chłodzące wbudowane w poszczególne urządzenia systemowe są włączane i wyłączane w zależności od aktualnej temperatury urządzenia.
- Każdemu wywołaniu można przyporządkować sygnał gongu poprzedzający emisję i drugi sygnał emitowany na zakończenie wywołania.
- Funkcje cyfrowego przetwarzania sygnału audio realizowane są przez poszczególne urządzenia systemowe. W związku z tym rolą sterownika sieciowego jest zestawianie odpowiednich połączeń i sterowanie całością pracy systemu.
- System posiada wewnętrzny zegar czasu rzeczywistego.

- Sterownik sieciowy jest wyposażony w pamięć komunikatów cyfrowych. Pojemność pamięci jest uzależniona wyłącznie od pojemności karty pamięci flash. Odtwarzacz komunikatów cyfrowych może odtwarzać jednocześnie 4 komunikaty. Istnieje możliwość odsłuchu zapisanych komunikatów.
- Sterownik sieciowy ma możliwość jednoczesnego zestawiania łączy dla maks. 28 kanałów audio. Sterownik tak zestawia łącza, wykorzystując dynamiczną alokację kanałów, aby wyeliminować lub zminimalizować możliwość powstawania konfliktów między poszczególnymi wywołaniami.
- Sterownik sieciowy zapamiętuje do 200 komunikatów o błędach powstałych w systemie.
- Sterownik sieciowy może zostać dołączony do sieci lokalnej istniejącej już w danym obiekcie. W takim przypadku stan systemu może być monitorowany z autoryzowanych komputerów dołączonych do lokalnej sieci, jeśli użytkownicy wprowadzą odpowiednie nazwy użytkownika i hasła.
- W systemie można wykorzystywać niestandardowe stacje wywoławcze złożone z dostępnych elementów systemowych.
- Regulacja głośności tła muzycznego w poszczególnych strefach nagłośnieniowych odbywa się za pośrednictwem odpowiednio skonfigurowanej stacji wywoławczej.
- Regulacja głośności wywołań w poszczególnych strefach może być realizowana w sposób automatyczny (AVC) z wykorzystaniem zewnętrznych mikrofonów pomiarowych
- Wejścia sterujące mają możliwość nadzorowania poprawności działania kabli, które są do nich dołączone.
- Wejścia sterujące mogą być dowolnie rozmieszczone w systemie i ich działanie jest całkowicie programowalne.
- Wejścia sterujące można skonfigurować do pracy w trybach chwilowym (monostabilnym) i przełączanym (bistabilnym). Tryb jest wybierany za pośrednictwem oprogramowania konfigurującego.
- System jest wyposażony w szereg wyjść sterujących ulokowanych w całym obiekcie. Każde wyjście sterujące może być programowane indywidualnie i reagować na określone wywołanie lub awarię systemu.
- Lokalizacja wzmacniaczy mocy w systemie jest dowolna. Spełnione muszą być jedynie warunki dotyczące logicznych adresów systemowych przypisanych do poszczególnych urządzeń. W przypadku CDSO obowiązują wymagania normy EN54-16 oraz lokalne przepisy.
- Wzmacniacze mocy są wyposażone w wyjścia sterujące, które można tak zaprogramować, aby sterowały urządzeniami w strefach nagłośnieniowych obsługiwanych przez dany wzmacniacz. Może to być np. obsługa obwodów obejścia regulacji głośności.
- Wzmacniacze mocy są wyposażone w wejścia zasilania awaryjnego 48 VDC. Dostęp do tego rodzaju zasilania może być monitorowany.
- System mierzy temperaturę pracy wzmacniacza mocy. Komunikaty o przekroczeniu dopuszczalnych zakresów temperatur są przekazywane do sterownika sieciowego.
- Wszystkim strefom nagłośnieniowym są przyporządkowane indywidualne kanały wzmacniaczy mocy.
- Istnieje możliwość konfiguracji systemu w trybie off-line (w czasie, kiedy system jest wyłączony). Umożliwia to dokonywanie zmian w konfiguracji z wyprzedzeniem i

nowe zmiany mogą być wprowadzane do systemu, który nie pracuje. Ogranicza to możliwość występowania zakłóceń w pracy systemu.

- Istnieje możliwość monitorowania aktywności kapsuły mikrofonowej stacji wywoławczej.
- Do odsłuchu wyjściowego sygnału audio ze wzmacniacza mocy typu PAM można wykorzystać gniazdo słuchawkowe, w jakie wyposażony jest wzmacniacz. Domyślnie na wyświetlaczu wzmacniacza wyświetlane są wskazania miernika wysterowania VU.
- Wystąpieniu błędu systemowego towarzyszy sygnał dźwiękowy generowany przez brzęczyk dołączony do sterownika. Natychmiast po usunięciu błędu lub awarii system automatycznie przechodzi do stanu „awaria zlikwidowana" i może zostać zresetowany.
- Za pośrednictwem stacji wywoławczych można dokonywać wywołań selektywnych. Jeśli dane wywołanie zostanie częściowo zakłócone przez wywołanie o wyższym priorytecie, emisja w strefach, w których nie doszło do konfliktu, będzie kontynuowana.
- Adres klawiatury stacji wywoławczej jest tak ustalany, że w przypadku awarii możliwa jest jego szybka wymiana bez konieczności przeprogramowywania systemu.
- Jeśli makropolecenie wywoławcze (makro) zostanie wybrane za pomocą klawiatury, makro standardowo przypisane do przycisku mikrofonowego (PTT) zostaje zawieszone.
- Istnieje możliwość ponownego wybrania poprzedniego wywołania za pomocą przycisku Recall.
- Parametry konfiguracyjne mogą zostać bezpośrednio przesłane do komputera PC ze sterownika sieciowego.
- Parametry toru przetwarzania sygnału audio mogą być w czasie rzeczywistym korygowane za pośrednictwem elementów obsługi użytkownika.
- Sterownik sieciowy posiada możliwość rejestracji określonej liczby zdarzeń systemowych z podaniem nazwy urządzenia, skąd pochodził sygnał wyzwalający.
- Zmiany konfiguracji można wprowadzać w tle podczas normalnej pracy systemu. Nie dotyczy to regulacji parametrów toru przetwarzania sygnału audio w czasie rzeczywistym. Zmiany odniosą skutek po ich zapisaniu i ponownym uruchomieniu systemu.
- Użytkownik może przypisywać nazwy do zapisywanych komunikatów cyfrowych. Komunikaty cyfrowe są przechowywane w postaci plików .wav (44,1kHz, 16-bit)
- Do danego przycisku wyboru można przypisać kilka komunikatów cyfrowych, razem z odpowiednimi funkcjami określającymi działanie odpowiednich wyjść i przycisku mikrofonowego.
- Istnieje możliwość utworzenia makrodefinicji wywołania, która jest połączeniem czynności wywoławczych, własności i przeznaczenia i którą można wywoływać za pośrednictwem dowolnej stacji wywoławczej lub wejścia sterującego.
- Rodzaj wejścia audio (liniowe / mikrofonowe) określa się za pomocą oprogramowania konfiguracyjnego.
- Głośność tła muzycznego może zostać ustalona indywidualnie dla każdej strefy.
- W pliku rejestru zapisywanym w komputerze PC odnotowywane są wszystkie wywołania łącznie z datą i czasem, modułem inicjującym, szczegółami dotyczącymi przycisku sterującego i przeznaczeniu wywołania.

- Pliki sterownika sieciowego, w których rejestrowane są błędy i zdarzenia systemowe, są typu pierścieniowego, a więc nie wymagają żadnej obsługi.
- Za pośrednictwem alarmowej stacji wywoławczej można rozszerzyć emisję bieżącego wywołania o nowe strefy nagłośnieniowe.
- Komunikaty alarmowe mogą być emitowane również w przypadku awarii sterownika sieciowego.
- System może umożliwiać rejestrację wywołań do stref uprzednio zajętych
- System może umożliwiać rejestrację wywołania i emisję po zakończeniu rejestracji w celu unikania sprzężeń akustycznych
- System może umożliwiać rejestrację wywołania celem wstępnego odsłuchania
- Dostęp do stacji wywoławczych komercyjnych może być ograniczony dla tylko osób znających kod autoryzacyjny
- Zakres dostępnych poziomów priorytetów od 0 do 255.

Opis głównych elementów systemu

a) Wielokanałowy interfejs BOSCH PRS-16MCI

- Interfejs podstawowych wzmacniaczy mocy
- Obsługa 16 kanałów audio do obsługi maks. 14 wzmacniaczy głównych (stref) oraz 2 wzmacniaczy rezerwowych
- Złącze nadmiarowej sieci optycznej
- Złącze wejść i wyjść sterujących
- Kompletny nadzór nad poprawnością działania własnej pracy oraz dołączonych wzmacniaczy podstawowych
- Złącza przelotowe wejść i wyjść sterujących , interfejs obsługuje bezpieczny tryb awaryjny, w którym wywołania alarmowe są przesyłane nawet w przypadku uszkodzenia interfejsu
- Interfejs może zostać skonfigurowany do przełączania nadmiarowych grup A/B lub do obsługi okablowania dołączonych wzmacniaczy podstawowych w postaci pętli klasy A.
- Zgodność z IEC 60849
- 32 wejścia sterujące oraz 16 wyjść sterujących
- 28 kanałów dostępnych dla obsługiwanego systemu

PARAMETRY UŻYTKOWE	
Pasmo przenoszenia	-3 dB przy 20 Hz i 20 kHz
Stosunek sygnał / szum	>85 dBA (bez syg. Pilota)
Przesłuchy	< -80 dB (1kHz)
Zniekształcenia	<0,1% (1 kHz)
Wejście liniowe	1 (ominiecie XLR)
Wyjście liniowe	1 (przelotowe XLR)
Wyjście liniowe	16 x - RJ45 (w parach) - 0 dB (symetrycznie)
Wejścia sterujące	32 x - zaciski śrubowe (przekaźniki) o obciążalności 24V, 1 A
Pobór mocy	12VDC

b) Wzmacniacze BOSCH: PRS-1B500, PRS-2B250, PRS-4B125, PRS-8B060

c) Wzmacniacze: 1x500W, 2x250W, 4x125W, 8x60W,

- Wzmacniacze w klasie D o wysokiej sprawności
- Impulsowe zasilacze sieciowe
- Wejścia lokalnego sygnału audio
- Kompletny nadzór
- Zgodność z IE 60849
- Komunikaty o awariach są przekazywane do sterownika sieciowego za pośrednictwem interfejsu wielokanałowego
- Wzmacniacze podstawowe posiadają oddzielne złącza głośników grupy A i B dla każdej strefy nagłośnieniowej i obsługują okablowanie głośników w postaci pętli klasy A. Wzmacniacze powinny być montowane w szafie typu Rack19"

ZASILANIE SIECIOWE			
Pobór mocy [W]	**Pmax-3dB (poziom sygnału alarmowego)**	**Stan bezczynności (przy sygnale pilota 15V)**	**Tryb czuwania**
Wzmacniacz 1x500W	450	52	17
Wzmacniacz 2x250W	378	46	18
Wzmacniacz 4x125W	395	62	16
Wzmacniacz 8x60W	400	80	16
ZASILANIE REZERWOWE (Akumulatory)			
Pobór mocy [W]	**Pmax-3dB (poziom sygnału alarmowego)**	**Stan bezczynności (przy sygnale pilota 15V)**	**Tryb czuwania**
Wzmacniacz 1x500W	365	34	6
Wzmacniacz 2x250W	370	38	6
Wzmacniacz 4x125W	375	48	9
Wzmacniacz 8x60W	385	62	10

PARAMETRY UŻYTKOWE	
Pasmo przenoszenia	60 Hz - 19 kHz (-3dB) 80 Hz - 19 kHz (-3dB, dla wzmacniacza 8x60)
Stosunek sygnał / szum	>85 dBA (bez syg. Pilota)
Przesłuchy	< -70 dB (1kHz)
Zniekształcenia	<03% (1 kHz) przy 50% mocy znamionowej
Wejście liniowe	1 (ominiecie XLR)
Wyjście liniowe	1 (przelotowe XLR)
Wyjście liniowe	16 x - RJ45 (w parach) - 0 dB (symetrycznie)
Wejścia sterujące	32 x - zaciski śrubowe (przekaźniki) o obciążalności 24V, 1 A

d) Podstawowa stacja wywoławcza BOSCH LBB 4430/00

- Złącze sieci nadmiarowej
- Wskaźnik włączenia zasilania
- Sygnalizacja stanu / awarii
- Zróżnicowana sygnalizacja wywołań o wyższym i niższym priorytecie
- Nadzór nad poprawnością działania kapsuły mikrofonowej
- Podstawowa stacja wywoławcza jest wyposażona w limiter oraz filtr korekcyjny mowy o częstotliwości odcięcia 340 Hz zwiększający zrozumiałość emitowanych komunikatów i zapobiegającemu przesterowaniom w zakresie niskich częstotliwości.
- Możliwość dołączenia maks. 16 modułów klawiatury za pośrednictwem łącza szeregowego. Klawiatury są zasilane ze stacji wywoławczej.
- Regulator głośności sygnału w głośniku odsłuchowym i zestawie nagłownym.
- Możliwość zaprogramowana klawiatury, aby wywołać chwilowe zwarcie lub na zmianę zwieranie i rozwierane (bez powtórzeń) styków sterujących w module głównym.
- Stacji można przyporządkować jeden z 224 poziomów priorytetów.
- W stacji odbywa się konwersja analogowego sygnału audio w sygnał cyfrowy.
- Cyfrowy procesor sygnałowy realizujący funkcje regulacji czułości wejściowej, układu limitera i korektora parametrycznego.
- Głośnik odsłuchowy włącza się, gdy dana stacja rozpoczyna emisję sygnału gongu lub zapisanego wcześniej komunikatu cyfrowego.

e) Rozdzielacz sieciowy BOSCH PRS-NSP

- 2 odczepy magistrali z ograniczeniem prądowym
- Obsługuje okablowanie nadmiarowe w pętli głównej
- Może dostarczać zasilanie z zewnętrznego zasilacza do sieci systemowej
- Wskaźniki do sygnalizacji zasilania i stanu awarii

f) Rozdzielacz sieciowy BOSCH PRS-FIN

- Nadmiarowe złącze sieciowe
- Wskaźniki do sygnalizacji zasilania i stanu awarii
- Dwa nadzorowane wejścia sterujące (nie PRS-FINNA)
- Możliwość korzystania z lokalnego zasilacza Sieciowego

g) Głośnik sufitowy BOSCH LC1-WM06E8 + osłona przeciwpożarowa LC1-MFD

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

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°

h) Głośnik ścienny BOSCH LBC 3018/01

	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

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°

i) Głośnik tubowy BOSCH LBC 3482/00

Czułość pasma oktawowego:

	SPL pasma oktawowego	Całkowite SPL pasma oktawowego	Całkowite SPL pasma oktawowego
	1 W / 1 m	1 W / 1 m	Pmax / 1 m
125 Hz	60,1		
250 Hz	86,6		
500 Hz	100,2		
1000 Hz	106,9		
2000 Hz	104,1		
4000 Hz	99,4		
8000 Hz	87,8		
A-ważone		100,1	113
Lin-ważone		99,8	111,8

Kąty promieniowania pasma oktawowego:

	W poziomie	W pionie
125 Hz		
250 Hz	360	360
500 Hz	120	120
1000 Hz	75	75
2000 Hz	43	43
4000 Hz	25	25
8000 Hz	22	22

Moc maksymalna:	37,5W
Moc znamionowa (PHC):	25/12,5/6,25
Poziom ciśnienia akustycznego przy mocy 25W/1W (1kHz,1m):	121dB/ 107dB
Efektywne pasmo przenoszenia (-10dB):	550Hz – 5kHz
Kąt promieniowania przy 1kHz/4kHz (-6db):	70°/25°
Napięcie znamionowe:	100V
Impedancja znamionowa:	4008Ω
Temperatura pracy:	-25° do 55°

j) Zasilacz z pomiarem rezystancji obwodu bateryjnego do DSO Praesideo ZDSO400E

Zasilacze dźwiękowych systemów ostrzegawczych ZDSO400E-AK3 jest kompletnym systemem zasilania z podtrzymaniem bateryjnym 48V dla dźwiękowego systemu ostrzegawczego Praesideo firmy Bosch.

Zasilacze posiadają świadectwo dopuszczenia CNBOP nr 1438/CPD/0213.

Konstrukcja oparta jest o standardową szafę w systemie 19". Oprócz zasilania w szafie zabudowuje się elementy systemu DSO (wzmacniacze, kontroler i inne). System zasilania, poza zapewnieniem zasilania sieciowego (głównego) dostarcza także zasilanie rezerwowe 48V z własnych baterii akumulatorów, które są chronione przed głębokim rozładowaniem. W każdym z obwodów bateryjnych nadzorowana jest wartość rezystancji, a przekroczenie zadeklarowanej wartości granicznej jest sygnalizowane.

Możliwe jest stosowanie pojedynczej szafy jak i zespołu kilku szaf. W celu zwiększenia prądu ładowania baterii akumulatorów lub podniesienia niezawodności pracy systemu do każdego zasilacza głównego można dołączyć zasilacz dodatkowy typu ZDSOR-400-E. W celu jednoczesnego podniesienia prądu ładowania i zwiększenia ilości dostępnych wyjść do zasilania modułów DSO można dołączyć zasilacz dodatkowy typu ZDSOT-400-E.

- zgodność z PN-EN 54 -4/A2
- zabudowa w szafie systemu 19"
- wysokość użytkowa szafy do 50 U (2 200 mm)

- zasilanie 1 fazowe lub 3 fazowe
- możliwość ustawienia szafy na kółkach, stopkach lub cokole
- podłączenia wykonywane poprzez dno szafy lub z tyłu przez przepust
- uzależnienie napięcia pracy buforowej od temperatury
- prowadzenie ładowania przyśpieszonego baterii z ograniczeniem prądu ładowania
- wymuszone chłodzenie wnętrza szafy

Funkcje urządzenia:

- rozprowadzenie zasilania sieciowego na moduły systemu DSO
- zabezpieczenie przepięciowe zasilania sieciowego
- zapewnienie napięcia gwarantowanego 48V
- rozprowadzenie napięcia 48V
- ładowanie, nadzorowanie i ochrona baterii akumulatorów
- ochrona baterii przed zbyt głębokim rozładowaniem
- kontrola rezystancji obwodów baterii w każdym ciągu bateryjnym
- kontrola stanu bezpieczników wyjść 48V dla wszystkich modułów DSO
- opcjonalna możliwość zapewnienie napięcia rezerwowego 230V (sinus) dla kontrolera LBB4401 sieci DSO (standardowo kontroler PRS-NCO-B z wejściem 48Vdc)
- generowanie alarmu w przypadku wykrycia błędów w pracy systemu

Wyposażenie:

- szafa 19” o wysokości i wielkości zależnej od indywidualnych wymagań DSO
- jedna, dwie lub trzy baterie akumulatorów 48V o pojemności zależnej od wymagań DSO
- miernik rezystancji obwodu baterii RMB-1
- przekładniki prądowe CP-100 - 1 szt. na każdą baterię akumulatorów
- zasilacz ZDSO-400-E wraz z sondą temperaturową i układem PFC oraz ew. zasilacz dodatkowy
- podsufitowy panel wentylatorów z wyłącznikiem termicznym (nie montowany w najmniejszych systemach)
- 1 lub 3 fazowe listwy zasilania sieciowego do podłączenia modułów DSO (ilość zależy od wielkości systemu)
- panel dystrybucji napięć z zabezpieczeniami obwodów baterii akumulatorów i obwodów sieciowych, zespołem ochrony przepięciowej oraz zaciskami alarmów systemu i alarmów zewnętrznych
- gniazdo serwisowe 230V
- przepust w tylnych drzwiach szafy

k) Zasilacz dodatkowy ZDZOR-400-E lub ZDSOT-400-E

Wielkość systemu		**Ogólnie**	
Rodzaj szafy 19"	600x600 (lub 800x600)	Zakres temperatur pracy	-5…40°C
Wysokość użytkowa szafy	min 24U max 50U	Chłodzenie	wymuszone
Ilość wzmacniaczy DSO Praesideo	max 8 [*]	Stopień ochrony	IP30
Zasilanie podstawowe (sieciowe)		Wymiary całkowite dla szafy 45U (W×S×G)	2180 × 600 × 600 mm
Przyłącze sieci 230V	1 lub 3 fazowe		
Zabezpieczenie przepięciowe przyłącza sieci	klasa III (D) 3kA	Masa po zainstalowaniu	~500kg [**]
Zasilanie rezerwowe (bateryjne)		**Zgodność z normami**	
Ilość baterii akumulatorów w systemie	1, 2 lub 3	Bezpieczeństwo elektryczne	PN-EN 60950-1:2007/A1:2011 kl. I
Maksymalna, łączna pojemność baterii akumulatorów	430 Ah	Zaburzenia radioelektryczne	PN-EN 55022 poziom B
Typ zasilacza ładującego i nadzorującego baterię aku.	ZDSO-400-E	Funkcjonalność	PN-EN 12101-10:2007
Maksymalny prąd ładowania	8A		
Czas podtrzymania napięcia rezerwowego 48V	6h lub 24h [**]		
Dopuszczalna rezystancja każdego z obwodów baterii	50…150mΩ [***]	Odporność EMC	PN-EN 50130-4:2012

* *Dodatkowy zasilacz ZDSOT-400-E posiada kolejnych 8 wyjść, przy czym całkowita ilość wzmacniaczy ograniczona jest wielkością szafy*
** *Przyjęto szafę 600x600mm o wysokości 42U zawierająca 6 wzmacniaczy i 2 baterie akumulatorów po 110Ah*
****Zależnie od konkretnego wykonania (m.in. wysokości szafy, ilości i pojemności baterii).*

Wytyczne dla inwestora, użytkownika i wykonawcy

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,
- dokumentację techniczną (powykonawczą) systemu zawierającą opis jego działania, sposób zasilania, umożliwiającą łatwą identyfikację linii głośnikowych, stref, objętych pomieszczeń oraz innych elementów systemu.

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,
- 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.

Poniżej przedstawiono przykładowe obliczenia systemów zasilania poszczególnych szaf DSO (Generalny Wykonawca zobowiązany jest wykonać na etapie realizacji aktualne obliczenia w oparciu o dane Producenta systemu zasilania zaakceptowanych przez Inwestora i Nadzór Autorski):

Szafa DSO1:

System zasilania **ZDSO400E-AK3** do DSO PRAESIDEO

3.000.13 (06-2017)

producent: MERAWEX

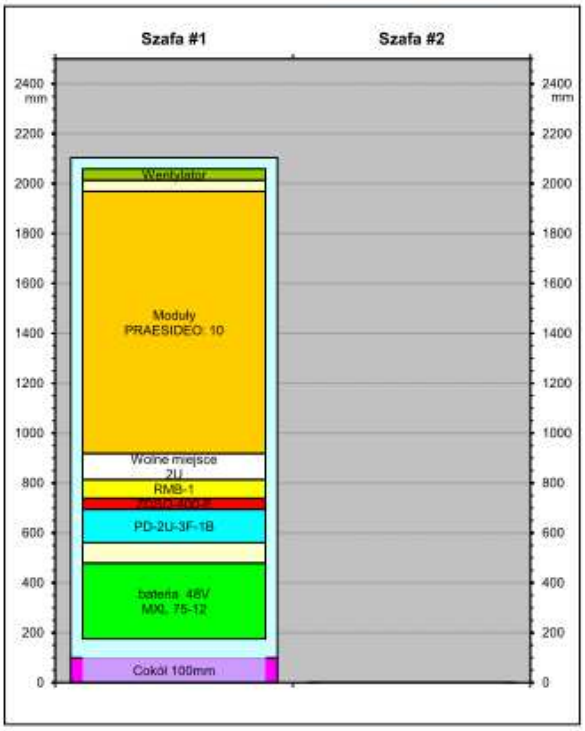
MERAWEX Sp. z o.o.
ul.Toruńska 8
44-122 GLIWICE

odbiorca (zamawiający):	wpisać nazwę firmy i oddział
specyfikacja do zamówienia nr:	
dla firmy:	
Miejsce instalacji:	
Adres:	
Osoba kontaktowa (odbierająca):	
Telefon do osoby kontaktowej:	
przewidywany termin realizacji:	2018-07-04
Data bieżąca:	18-8-2019

Zasilanie awaryjne	48	Vdc
Czas oczekiwania	6	h
Czas alarmu	0,5	h

Maksymalna moc wyjściowa systemu: 3000 W

Moduły DSO systemu: ○PRAESIDEO 2 ◉PRAESIDEO 3	Typ	Szafa: Szafa #1	Szafa #2
Kontroler			
Kontroler sieci (230Vac/48Vdc)	PRS-NCO-B		
Urządzenia dodatkowe - zasilanie tylko z sieci 230Vac			
Amplituner +CD (BGM Source)	PLE-SDT		
Urządzenia w szafach zasilane z kontrolera sieci			
Audio ekspander (audio expander)	PRS-4AEX4		
INTERFEJS wielokanałowy	PRS-16-MCI	2	
Urządzenia poza szafami zasilane z kontrolera sieci			
Stacja wywoławcza (call station)	LBB4430,PRS-CSI	1	
Klawiatura stacji wywoławczej (keypad)	LBB4432,PRS-CSNKP	1	
Rozdzielnica sieci optycznej (splitter)	LBB4410, PRS-NSP		
Interfejs optyczny (fibre interface)	LBB4414, PRS-FINxx	2	
Zasilanie z sieci lub 48V			
Wzmacniacz mocy 1x500W	PRS-1P500		
Zapas			
Wzmacniacz mocy 2x250W	PRS-2P250		
Zapas			
Wzmacniacz mocy 4x125W	PRS-4P125		
Zapas			
Wzmacniacz mocy 8x60W	LBB 4428/00		
Zapas			
Wzmacniacz podstawowy 1x500W	PRS-1B500		
Zapas		2	
Wzmacniacz podstawowy 2x250W	PRS-2B250	2	
Zapas			
Wzmacniacz podstawowy 4x125W	PRS-4B125	3	
Zapas			
Wzmacniacz podstawowy 8x60W	PRS-8B060	1	
Zapas			
Ilość modułów	Razem:	10	
Dodatkowe miejsce w szafie (zapas)	U		



Pojemność akumulatorów -obliczeniowa (minimalna):	71Ah	
Baterie akumulatorów	☑ ☐	☐ ☐
Dobór pojemności baterii akumulatorów		
kontaż w układzie gniazda	MXL 75-12 C20=82Ah	
Nadwyżka pojemności	Ah 11,8	
Prąd ładowania 24h	A 3,5	
Zasilacze ZDSO-400-E	☑	☐
Dodatkowy ZDSOT-400-E	☐	☐
Redundancja ZDSOR-400-E	☐	☐

Wielkość szafy 42U (600x800)
Podstawa: Cokół 100mm

Wybór przyłącza sieci: 3 fazowe
Prąd nominalny (fazowy) 10 A
Zabezpieczenie główne 16 A

Dane potrzebne w celu ustalenia ceny w cenniku:
szafa: **42U (600x800)**
akumulatory: **1 x MXL 75-12 - 1 półka**

Całkowity prąd baterii akumulatorów		
w czasie oczekiwania	A	6,2
w czasie alarmu	A	26,3
maksymalna wartość chwilowa	A	75,7

Waga transportowa	Szafa #1	Szafa #2	
Szafa bez modułów PRAESIDEO	177	0	kg
Akumulatory	92	0	kg
Całość	**269**	**0**	**kg**
Waga instalacyjna			
Moduły PRAESIDEO	125	0	kg
Całość	**393**	**0**	**kg**

Zabezpieczenia obwodów:	Szafa #1	Szafa #2
- sieć	S304 C16	
- każda z baterii	D02 35A	
-zasilacze ZDSO-400-E	S301 C16	
- gniazdo serwisowe	S301 C2	

Średnia moc strat	Szafa #1	Szafa #2	
Łącznie	**807 W**	**807**	**0**	**W**

Tabliczka znamionowa	Szafa #1	Szafa #2
Prądy maksymalne dla 184V	**3x 12**	**A**

Szafa DSO2:

System zasilania ZDSO400E-AK3 do DSO PRAESIDEO

3.000.13 (06-2017)

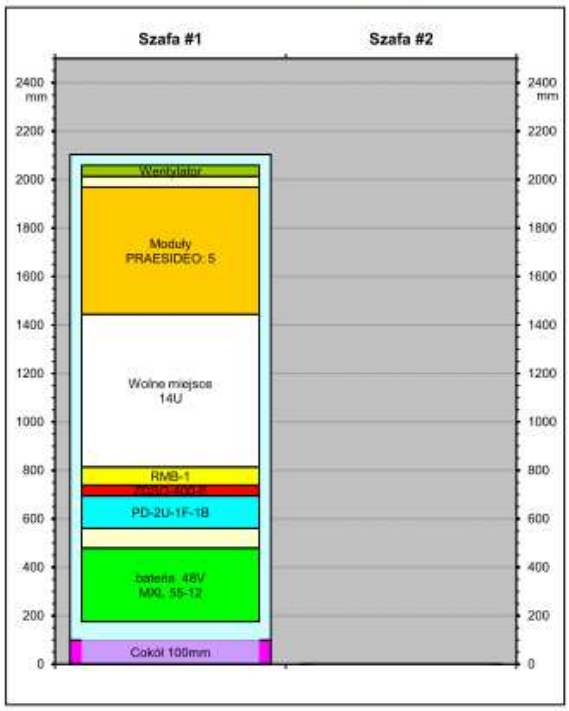
producent:
MERAWEX
MERAWEX Sp. z o.o.
ul.Toruńska 8
44-122 GLIWICE

odbiorca (zamawiający):	wpisać nazwę firmy i oddział
specyfikacja do zamówienia nr:	
dla firmy:	
Miejsce instalacji:	
Adres:	
Osoba kontaktowa (odbierająca):	
Telefon do osoby kontaktowej:	
przewidywany termin realizacji:	2018-07-04
Data bieżąca:	18-8-2019

Zasilanie awaryjne	48	Vdc
Czas oczekiwania	6	h
Czas alarmu	0,5	h

Maksymalna moc wyjściowa systemu: 1500 W

Moduły DSO systemu: ○PRAESIDEO 2 ◉PRAESIDEO 3	Typ	Szafa: Szafa #1	Szafa #2
Kontroler			
Kontroler sieci (230Vac/48Vdc)	PRS-NCO-B		
Urządzenia dodatkowe - zasilanie tylko z sieci 230Vac			
Amplituner +CD (BGM Source)	PLE-SDT		
Urządzenia w szafach zasilane z kontrolera sieci			
Audio ekspander (audio expander)	PRS-4AEX4		
INTERFEJS wielokanałowy	PRS-16-MCI	1	
Urządzenia poza szafami zasilane z kontrolera sieci			
Stacja wywoławcza (call station)	LBB4430,PRS-CSI	1	
Klawiatura stacji wywoławczej (keypad)	LBB4432,PRS-CSNKP	1	
Rozdzielnica sieci optycznej (splitter)	LBB4410, PRS-NSP		
Interfejs optyczny (fibre interface)	LBB4414, PRS-FINxx	2	
Zasilanie z sieci lub 48V			
Wzmacniacz mocy 1x500W	PRS-1P500		
Zapas			
Wzmacniacz mocy 2x250W	PRS-2P250		
Zapas			
Wzmacniacz mocy 4x125W	PRS-4P125		
Zapas			
Wzmacniacz mocy 8x60W	LBB 4428/00		
Zapas			
Wzmacniacz podstawowy 1x500W	PRS-1B500		
Zapas		1	
Wzmacniacz podstawowy 2x250W	PRS-2B250		
Zapas			
Wzmacniacz podstawowy 4x125W	PRS-4B125	2	
Zapas			
Wzmacniacz podstawowy 8x60W	PRS-8B060	1	
Zapas			
Ilość modułów	Razem:	5	
Dodatkowe miejsce w szafie (zapas)	U		



Baterie akumulatorów	Pojemność akumulatorów -obliczeniowa (minimalna):	41Ah	
		☑	☐ ☐
		☐	☐ ☐

Dobór pojemności baterii akumulatorów: MXL 55-12 C20=60Ah

Nadwyżka pojemności		Ah	19,5
Prąd ładowania 24h		A	2,5
Zasilacze	ZDSO-400-E		☑ ☐
Dodatkowy	ZDSOT-400-E		☐ ☐
Redundancja	ZDSOR-400-E		☐ ☐

Całkowity prąd baterii akumulatorów		
w czasie oczekiwania	A	3,7
w czasie alarmu	A	13,9
maksymalna wartość chwilowa	A	40,8

Zabezpieczenia obwodów:	Szafa #1	Szafa #2
- sieć	S302 C16	
- każda z baterii	D02 25A	
-zasilacze ZDSO-400-E	S301 C16	
- gniazdo serwisowe	S301 C2	

Tabliczka znamionowa	Szafa #1	Szafa #2
Prądy maksymalne dla 184V	1x 16	A

Wielkość szafy: 42U (600x800)
Podstawa: Cokół 100mm

Wybór przyłącza sieci: 1 fazowe — Prąd nominalny (fazowy) 13 A; Zabezpieczenie główne 16 A

Dane potrzebne w celu ustalenia ceny w cenniku:
szafa: 42U (600x800)
akumulatory: 1 x MXL 55-12 - 1 półka

Waga transportowa	Szafa #1	Szafa #2	
Szafa bez modułów PRAESIDEO	173	0	kg
Akumulatory	71	0	kg
Całość	244	0	kg
Waga instalacyjna			
Moduły PRAESIDEO	63	0	kg
Całość	307	0	kg

Średnia moc strat	Szafa #1	Szafa #2	
Łącznie	457 W	457	0 W

Szafa DSO3:

System zasilania **ZDSO400E-AK3** do DSO PRAESIDEO

3.000.13 (06-2017)

producent: MERAWEX

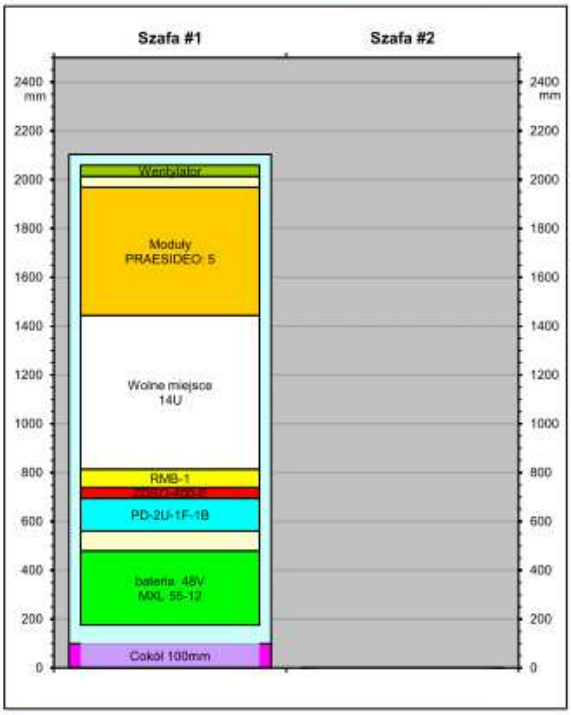
MERAWEX Sp. z o.o.
ul.Toruńska 8
44-122 GLIWICE

odbiorca (zamawiający):	wpisać nazwę firmy i oddział
specyfikacja do zamówienia nr:	
dla firmy:	
Miejsce instalacji:	
Adres:	
Osoba kontaktowa (odbierająca):	
Telefon do osoby kontaktowej:	
przewidywany termin realizacji:	2018-07-04
Data bieżąca:	18-8-2019

Zasilanie awaryjne	48	Vdc
Czas oczekiwania	6	h
Czas alarmu	0,5	h

Maksymalna moc wyjściowa systemu: **1500 W**

Moduły DSO systemu: ○PRAESIDEO 2 ●PRAESIDEO 3	Typ	Szafa: Szafa #1	Szafa #2
Kontroler			
Kontroler sieci (230Vac/48Vdc)	PRS-NCO-B		
Urządzenia dodatkowe - zasilanie tylko z sieci 230Vac			
Amplituner +CD (BGM Source)	PLE-SDT		
Urządzenia w szafach zasilane z kontrolera sieci			
Audio ekspander (audio expander)	PRS-4AEX4		
INTERFEJS wielokanałowy	PRS-16-MCI	1	
Urządzenia poza szafami zasilane z kontrolera sieci			
Stacja wywoławcza (call station)	LBB4430,PRS-CSI	1	
Klawiatura stacji wywoławczej (keypad)	LBB4432,PRS-CSNKP	1	
Rozdzielnica sieci optycznej (splitter)	LBB4410, PRS-NSP		
Interfejs optyczny (fibre interface)	LBB4414, PRS-FINxx	2	
Zasilanie z sieci lub 48V			
Wzmacniacz mocy 1x500W	PRS-1P500		
Zapas			
Wzmacniacz mocy 2x250W	PRS-2P250		
Zapas			
Wzmacniacz mocy 4x125W	PRS-4P125		
Zapas			
Wzmacniacz mocy 8x60W	LBB 4428/00		
Zapas			
Wzmacniacz podstawowy 1x500W	PRS-1B500		
Zapas		1	
Wzmacniacz podstawowy 2x250W	PRS-2B250	1	
Zapas			
Wzmacniacz podstawowy 4x125W	PRS-4B125	1	
Zapas			
Wzmacniacz podstawowy 8x60W	PRS-8B060	1	
Zapas			
Ilość modułów	Razem:	5	
Dodatkowe miejsce w szafie (zapas)	U		



Pojemność akumulatorów -obliczeniowa (minimalna):	39Ah	
Baterie akumulatorów		
Dobór pojemności baterii akumulatorów	MXL 55-12 C20=60Ah	
Nadwyżka pojemności	Ah	21,3
Prąd ładowania 24h	A	2,5
Zasilacze	ZDSO-400-E	☑
Dodatkowy	ZDSOT-400-E	☐
Redundancja	ZDSOR-400-E	☐

Wielkość szafy	42U (600x800)	
Podstawa:	Cokół 100mm	

Wybór przyłącza sieci:	1 fazowe	
Prąd nominalny (fazowy)	13 A	
Zabezpieczenie główne	16 A	

Dane potrzebne w celu ustalenia ceny w cenniku:
szafa: **42U (600x800)**
akumulatory: **1 x MXL 55-12 - 1 półka**

Całkowity prąd baterii akumulatorów		
w czasie oczekiwania	A	3,6
w czasie alarmu	A	13,7
maksymalna wartość chwilowa	A	38,7

Waga transportowa	Szafa #1	Szafa #2	
Szafa bez modułów PRAESIDEO	173	0	kg
Akumulatory	71	0	kg
Całość	**244**	**0**	**kg**
Waga instalacyjna			
Moduły PRAESIDEO	62	0	kg
Całość	**306**	**0**	**kg**

Zabezpieczenia obwodów:	Szafa #1	Szafa #2
- sieć	S302 C16	
- każda z baterii	D02 25A	
-zasilacze ZDSO-400-E	S301 C16	
- gniazdo serwisowe	S301 C2	

Średnia moc strat	Szafa #1	Szafa #2	
Łącznie	445 W	445	0 W

Tabliczka znamionowa	Szafa #1	Szafa #2
Prądy maksymalne dla 184V	1x 16	A

Szafa DSO4:

System zasilania ZDSO400E-AK3 do DSO PRAESIDEO

3.000.13 (06-2017)

producent: MERAWEX

MERAWEX Sp. z o.o.
ul.Toruńska 8
44-122 GLIWICE

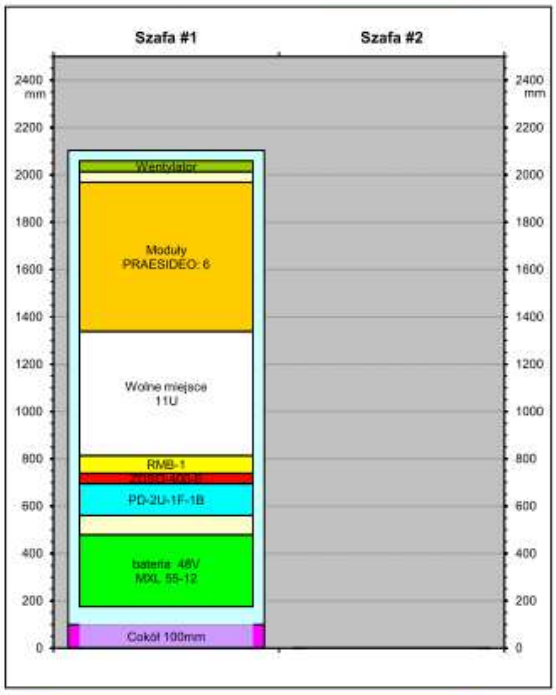
odbiorca (zamawiający):	wpisać nazwę firmy i oddział
specyfikacja do zamówienia nr:	
dla firmy:	
Miejsce instalacji:	
Adres:	
Osoba kontaktowa (odbierająca):	
Telefon do osoby kontaktowej:	
przewidywany termin realizacji:	2018-07-04 Data bieżąca: 18-8-2019

Zasilanie awaryjne	48	Vdc
Czas oczekiwania	6	h
Czas alarmu	0,5	h

Maksymalna moc wyjściowa systemu: 2000 W

Moduły DSO systemu: ○PRAESIDEO 2 ◉PRAESIDEO 3

Typ	Szafa: Szafa #1	Szafa #2
Kontroler		
Kontroler sieci (230Vac/48Vdc) PRS-NCO-B		
Urządzenia dodatkowe - zasilanie tylko z sieci 230Vac		
Amplituner +CD (BGM Source) PLE-SDT		
Urządzenia w szafach zasilane z kontrolera sieci		
Audio ekspander (audio expander) PRS-4AEX4		
INTERFEJS wielokanałowy PRS-16-MCI	1	
Urządzenia poza szafami zasilane z kontrolera sieci		
Stacja wywoławcza (call station) LBB4430,PRS-CSI	1	
Klawiatura stacji wywoławczej (keypad) LBB4432,PRS-CSNKP	1	
Rozdzielnica sieci optycznej (splitter) LBB4410, PRS-NSP		
Interfejs optyczny (fibre interface) LBB4414, PRS-FINxx	2	
Zasilanie z sieci lub 48V		
Wzmacniacz mocy 1x500W PRS-1P500 Zapas		
Wzmacniacz mocy 2x250W PRS-2P250 Zapas		
Wzmacniacz mocy 4x125W PRS-4P125 Zapas		
Wzmacniacz mocy 8x60W LBB 4428/00 Zapas		
Wzmacniacz podstawowy 1x500W PRS-1B500 Zapas	1	
Wzmacniacz podstawowy 2x250W PRS-2B250 Zapas	2	
Wzmacniacz podstawowy 4x125W PRS-4B125 Zapas	2	
Wzmacniacz podstawowy 8x60W PRS-8B060 Zapas		
Ilość modułów Razem	6	
Dodatkowe miejsce w szafie (zapas) U		



Baterie akumulatorów

Pojemność akumulatorów -obliczeniowa (minimalna): 43Ah

Dobór pojemności baterii akumulatorów

MXL 55-12 C20=60Ah

Nadwyżka pojemności		Ah	17,4
Prąd ładowania 24h		A	2,5
Zasilacze	ZDSO-400-E		☑ ☐
Dodatkowy	ZDSOT-400-E		☐ ☐
Redundancja	ZDSOR-400-E		☐ ☐

Wielkość szafy 42U (600x800)
Podstawa: Cokół 100mm

Wybór przyłącza sieci: 1 fazowe Prąd nominalny (fazowy) 16 A
Zabezpieczenie główne 20 A

Dane potrzebne w celu ustalenia ceny w cenniku:
szafa: 42U (600x800)
akumulatory: 1 x MXL 55-12 - 1 półka

Całkowity prąd baterii akumulatorów		
w czasie oczekiwania	A	3,7
w czasie alarmu	A	17
maksymalna wartość chwilowa	A	48,3

Waga transportowa	Szafa #1	Szafa #2	
Szafa bez modułów PRAESIDEO	174	0	kg
Akumulatory	71	0	kg
Całość	**245**	**0**	**kg**
Waga instalacyjna			
Moduły PRAESIDEO	77	0	kg
Całość	**322**	**0**	**kg**

Zabezpieczenia obwodów:	Szafa #1	Szafa #2
- sieć	S302 C20	
- każda z baterii	D02 25A	
-zasilacze ZDSO-400-E	S301 C16	
- gniazdo serwisowe	S301 C2	

Średnia moc strat		Szafa #1	Szafa #2	
Łącznie	505 W	505	0	W

Tabliczka znamionowa	Szafa #1	Szafa #2
Prądy maksymalne dla 184V	1x 19,5	A

Szafa DSO5:

System zasilania ZDSO400E-AK3 do DSO PRAESIDEO

3.000.13 (06-2017)

producent:
MERAWEX
MERAWEX Sp. z o.o.
ul.Toruńska 8
44-122 GLIWICE

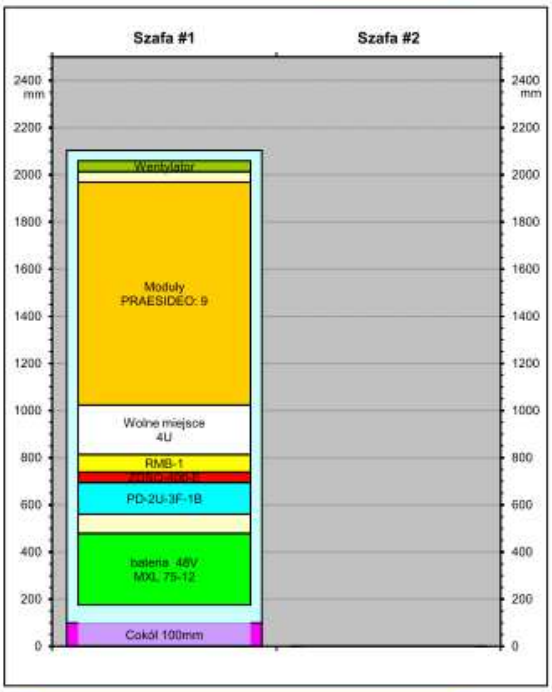
odbiorca (zamawiający):	wpisać nazwę firmy i oddział
specyfikacja do zamówienia nr:	
dla firmy:	
Miejsce instalacji:	
Adres:	
Osoba kontaktowa (odbierająca):	
Telefon do osoby kontaktowej:	
przewidywany termin realizacji:	2018-07-04 Data bieżąca: 18-8-2019

Zasilanie awaryjne	48	Vdc
Czas oczekiwania	6	h
Czas alarmu	0,5	h

Maksymalna moc wyjściowa systemu: 2500 W

Moduły DSO systemu: ○PRAESIDEO 2 ◉PRAESIDEO 3

Typ	Szafa: Szafa #1	Szafa #2
Kontroler		
Kontroler sieci (230Vac/48Vdc) PRS-NCO-B		
Urządzenia dodatkowe - zasilanie tylko z sieci 230Vac		
Ampltuner +CD (BGM Source) PLE-SDT		
Urządzenia w szafach zasilane z kontrolera sieci		
Audio ekspander (audio expander) PRS-4AEX4		
INTERFEJS wielokanałowy PRS-16-MCI	2	
Urządzenia poza szafami zasilane z kontrolera sieci		
Stacja wywoławcza (call station) LBB4430,PRS-CSI	1	
Klawiatura stacji wywoławczej (keypad) LBB4432,PRS-CSNKP	1	
Rozdzielnica sieci optycznej (splitter) LBB4410, PRS-NSP		
Interfejs optyczny (fibre interface) LBB4414, PRS-FINxx	2	
Zasilanie z sieci lub 48V		
Wzmacniacz mocy 1x500W PRS-1P500		
Zapas		
Wzmacniacz mocy 2x250W PRS-2P250		
Zapas		
Wzmacniacz mocy 4x125W PRS-4P125		
Zapas		
Wzmacniacz mocy 8x60W LBB 4428/00		
Zapas		
Wzmacniacz podstawowy 1x500W PRS-1B500		
Zapas	2	
Wzmacniacz podstawowy 2x250W PRS-2B250	1	
Zapas		
Wzmacniacz podstawowy 4x125W PRS-4B125	2	
Zapas		
Wzmacniacz podstawowy 8x60W PRS-8B060	2	
Zapas		
Ilość modułów Razem:	9	
Dodatkowe miejsce w szafie (zapas) U		



Pojemność akumulatorów -obliczeniowa (minimalna): 67Ah

Baterie akumulatorów

Dobór pojemności baterii akumulatorów
montaż w układzie gniazda: MXL 75-12 C20=82Ah

Nadwyżka pojemności	Ah	15,9	
Prąd ładowania 24h	A	3,5	
Zasilacze	ZDSO-400-E	☑	☐
Dodatkowy	ZDSOT-400-E	☐	☐
Redundancja	ZDSOR-400-E	☐	☐

Wielkość szafy 42U (600x800)
Podstawa: Cokół 100mm

Wybór przyłącza sieci: 3 fazowe — Prąd nominalny (fazowy) 10 A; Zabezpieczenie główne 16 A

Dane potrzebne w celu ustalenia ceny w cenniku:
szafa: 42U (600x800)
akumulatory: 1 x MXL 75-12 - 1 półka

Całkowity prąd baterii akumulatorów		
w czasie oczekiwania	A	6
w czasie alarmu	A	23
maksymalna wartość chwilowa	A	66,2

Waga transportowa	Szafa #1	Szafa #2	
Szafa bez modułów PRAESIDEO	176	0	kg
Akumulatory	92	0	kg
Całość	**268**	**0**	**kg**
Waga instalacyjna			
Moduły PRAESIDEO	109	0	kg
Całość	**377**	**0**	**kg**

Zabezpieczenia obwodów:	Szafa #1	Szafa #2
- sieć	S304 C16	
- każda z baterii	D02 25A	
-zasilacze ZDSO-400-E	S301 C16	
- gniazdo serwisowe	S301 C2	

Średnia moc strat	Szafa #1	Szafa #2	
Łącznie	747 W	747	0 W

Tabliczka znamionowa	Szafa #1	Szafa #2	
Prądy maksymalne dla 184V	3x 12		A

5.5 Stałe urządzenia gaśnicze

Zgodnie z postanowieniem WZ-5595-3/12 Łódzkiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej w Łodzi, dotyczącego braku konieczności instalacji stałych samoczynnych urządzeń gaśniczych wodnych w wybranych pomieszczeniach, projektuje się wyposażenie tych pomieszczeń w stałe urządzenia gaśnicze gazowe. Systemem będą objęte nowoprojektowane pomieszczenia teletechniczne i elektryczne w budynku A1. Projekt nie jest przedmiotem tego opracowania i rozwiązania projektowe opisane zostały w tomie II części VIII.

5.6 Instalacja sieci strukturalnej

Przyłącze

Na potrzeby uzyskania dostępu do sieci teleinformatycznej przewiduje się wykorzystanie istniejącego przyłącza telekomunikacyjnego w istniejącej części szpitala. W tym celu do projektowanych BPD (Budynkowych Punktów Dystrybucyjnych – po jednym w budynku A1 oraz A2) projektuje się doprowadzenie minimum 24-włóknowego światłowodu jednomodowego SM OS2 24J. Światłowód będzie prowadzony z wykorzystaniem projektowanych oraz istniejących tras kablowych do budowanej obecnie nowej serwerowni szpitalnej w budynku A2. Należy zastosować standard złącz LC-LC.

Jako połączenie redundantne przewiduje się doprowadzenie minimum 24-włóknowego światłowodu jednomodowego SM OS2 24J do istniejącej serwerowni w budynku A1.

Opis systemu

Projektuje się Budynkowe Punkty Dystrybucyjne oraz Lokalne Punkty Dystrybucyjne. Przewiduje się wykonanie połączeń BPD-LPD w topologii gwiazdy z nadmiarowymi połączeniami pomiędzy poszczególnymi LPD. Opcjonalnie należy przewidzieć równoległe okablowanie miedziane. Każdy LPD będzie połączony z BPD oraz z minimum jednym sąsiednim LPD przy pomocy kabli światłowodowych jednomodowych. Należy zastosować standard złącz LC-LC.

Podsystem okablowania poziomego zostanie zrealizowany na bazie systemu ekranowanego F/FTP w kategorii 6A zgodnie z ISO/IEC 11801 oraz EN 50173-1. Minimalne wymagania elementów to kategoria 6A (komponenty)/klasa Ea (wydajność całego systemu). Należy wykorzystać kable w powłokach bezhalogenowych i trudnopalnych LSZH (LSOH).

Projektuje się minimum dwie fizycznie wydzielone sieci LAN: sieć na potrzeby ogólne oraz sieć przeznaczoną dla systemów budynkowych (CCTV, SKD, itp.).

W punktach dystrybucyjnych projektuje się wykorzystanie szaf RACK 19” 42U o minimalnych wymiarach 800 x 800 mm. W szafach należy zainstalować zarówno osprzęt pasywny okablowania strukturalnego, jak i sprzęt aktywny.

System sieci strukturalnej musi zapewniać możliwość podłączenia urządzeń komputerowych, urządzeń medycznych (np. na potrzeby monitorowania parametrów życiowych pacjentów), urządzeń technologicznych (np. na potrzeby systemu automatyki budynkowej), a także urządzeń stanowiących elementy systemów zabezpieczeń (np. kontrolery SKD, SSWiN, kamery).

Projektuje się minimum:

- jedno podwójne gniazdo RJ45 na każde stanowisko robocze w pomieszczeniach biurowych,
- jedno podwójne gniazdo RJ45 na stanowisko komputerowe w pomieszczeniach dydaktycznych (salach komputerowych),
- jedno podwójne gniazdo RJ45 na stanowisko komputerowe w pomieszczeniach dydaktycznych (aulach, salach wykładowych, seminaryjnych i ćwiczeniowych),
- jedno podwójne gniazdo RJ45 na stanowisko komputerowe w pomieszczeniach specjalistycznych.

W komunikacjach projektuje się dodatkowe przyłącza RJ45 instalowane pod sufitem na potrzeby bezprzewodowego dostępu do sieci.

Rozwiązania części pasywnej systemu muszą pochodzić z oferty od jednego producenta i być objęte jednolitą i spójną gwarancją systemową producenta na okres minimum 20 lat obejmującą wszystkie elementy pasywne toru transmisyjnego, jak również płyty czołowe gniazd końcowych, wieszaki kablowe i szafy dystrybucyjne. Wszystkie elementy pasywne składające się na okablowanie strukturalne muszą być oznaczone nazwą lub znakiem firmowym tego samego producenta okablowania i pochodzić z jednolitej oferty reprezentującej kompletny system w taki zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu gwarancyjnego w/w producenta.

W celu zagwarantowania jak najwyższych marginesów pracy i zapasów parametrów transmisyjnych nie dopuszcza się rozwiązań złożonych z elementów różnych producentów (tj. kabla, gniazd, paneli, kabli krosowych, itp.).

Wszystkie komponenty systemu okablowania muszą być zgodne z wymaganiami obowiązujących norm wg: ISO/IEC 11801, EN 50173-1, PN-EN 50173-1, IEC 61156-5, ANSI/TIA/EIA 568-B.2-1.

Wszystkie kable okablowania poziomego oznaczone zostaną w sposób umożliwiający ich łatwą identyfikację. Przyjęto następujący system oznaczeń kabli miedzianych okablowania poziomego:

XX/YY/ZZ

Gdzie: XX – nr punktu dystrybucyjnego, YY – nr patchpanelu, ZZ – nr portu.

Sposób numeracji gniazd należy w trakcie realizacji Inwestycji dostosować do aktualnie stosowanego przez Inwestora. Wszystkie oznaczenia należy nanieść na poszczególnych elementach systemu okablowania strukturalnego (na kablach, panelach i gniazdach) oraz wszystkich elementach instalacji teletechnicznych (okablowaniu i urządzeniach), a także wykaz tych oznaczeń należy zawrzeć w dokumentacji powykonawczej.

Urządzenia aktywne

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 odpowiednią platformę sprzętową i programową, w pełni ze sobą zintegrowaną, zapewniającą późniejsze 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 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 zarządzanie dostępem w zakresie sieci przewodowej, z uwzględnieniem jednolitych mechanizmów 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.

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, połączone przez współdzielony szkielet sieci LAN,

• 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 w budynkach A1 i A2 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, zintegrowane są per system, ale z uwzględnieniem:

- dla systemu bezpieczeństwa, zakłada się agregację połączeń 1Gb/s,

- dla pozostałych systemów, oparte o agregację połączeń 10Gb/s, 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 wspólnej 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 – BPD, w budynku A1, z uwzględnieniem wstępnie zakładanych wydajności i ilości jednocześnie zarządzanych urządzeń końcowych sieci. Wstępne założenia przedstawione są szczegółowo w dalszej części projektu.

8. System kontroli dostępu do sieci LAN jest oparty o system NAC (z odpowiednimi modułami funkcjonalnymi, opisanymi w dalszej części projektu), zintegrowany z pozostałymi systemami do kontroli/utrzymania/monitorowania sieci komputerowej w Szpitalu.

9. 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.

10. Warstwa kontroli poszczególnych punktów dostępu do sieci bezprzewodowej, oparta jest na redundantnym systemem kontrolera, w postaci zrytualizowanej, pracującym w trybie active/active, który będzie zainstalowany na serwerze.

11. 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.

12. 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.

Na potrzeby urządzeń aktywnych w tym instalacji HIS i PACS przewidziano odpowiednią ilość miejsca w szafach RACK oraz podtrzymanie zasilania na wypadek zaniku zasilania podstawowego.

Rezerwowanie danych

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

Szpitalny system informatyczny

Zakłada się wykorzystanie istniejących w szpitalu serwerów i licencji systemów HIS, nie przewiduje się ich rozbudowy.

System informacji wizualnej

Na potrzeby systemu informacji wizualnej DS. (ang. Digital Signage) przewidziano dedykowane gniazda RJ45. Ich lokalizacje wskazane zostały w części rysunkowej.

Okablowanie w salach AV

Na potrzeby sal seminaryjnych i innych objętych systemem AV, oprócz dedykowanych gniazd na potrzeby tego systemu (sparametryzowane w modelu) należy wykonać:

- dla sal w standardzie 1: ułożyć link miedziany z odpowiednimi zapasami instalacyjnymi w relacji przyłącze ścienne przy monitorze <->przyłącze ścienne przy biurku
- dla sal w standardzie 2:
    - ułożyć link miedziany z odpowiednimi zapasami instalacyjnymi w relacji przyłącze ścienne przy biurku <-> panel sterujący w biurku
    - ułożyć 3 linki miedziane w relacji przyłącze ścienne przy monitorze <-> przyłącze ścienne przy biurku
- dla sal w standardzie 3:
    - ułożyć link miedziany z odpowiednimi zapasami instalacyjnymi w relacji przyłącze ścienne przy biurku <-> panel sterujący

- ułożyć 3 linki miedziane w relacji przyłącze ścienne przy monitorze <->przyłącze ścienne przy biurku

- dla sali w standardzie 4:
  - ułożyć link miedziany z odpowiednimi zapasami instalacyjnymi w relacji panel sterujący przy ekranie głównym <-> szafa AV
  - ułożyć link miedziany z odpowiednimi zapasami instalacyjnymi w relacji przestrzeń sufitowa (lokalizacja AP) <-> szafa AV
  - Ułożyć po 3 linki miedziane z odpowiednimi zapasami instalacyjnymi w relacji rzutnik <-> szafa AV
  - Ułożyć 3 linki miedziane z odpowiednimi zapasami instalacyjnymi w relacji przyłącze ścienne <-> szafa AV
  - Ułożyć link miedziany z odpowiednimi zapasami instalacyjnymi w relacji rozdzielnica na potrzeby obsługi Sali <-> szafa AV

Zestawienie elementów sieci strukturalnej

LAN (PC, VoIP, WiFi, systemy informacyjne, IP TV itp.)											
						przełaczniki L2 (PC, VoIP, WiFi)					
poziom	Nazwa PD	nazwa szafy	linie RJ45	suma portów (z uwzgl. zapasu)	WiFi (2xRJ45)	24	48	panel 48xRJ45	wieszak 1U	wypełnienie szaf [U]	kable stakujące
P02	BPD-A2	BPD.1	152	207	20	1	4	5	5	15	5
P02	BPD-A2	BPD.2	0	0	0	0	0	0	0	0	0
P02	BPD-A2	BPD.3	0	0	0	0	0	0	0	0	0
P02	BPD-A2	BPD.4	0	0	0	0	0	0	0	0	0
P02	BPD-A2	BPD.5	0	0	0	0	0	0	0	0	0
P02	LPD-02.I-A2	P02.1	2	4	1	1	0	1	1	3	0
P02	LPD-02.I-A2	P02.2	0	0	0	0	0	0	0	0	0
P02	LPD-02.II-A2	P02.3	98	168	30	1	3	4	4	12	4
P02	LPD-02.II-A2	P02.4	0	0	0	0	0	0	0	0	0
P02	LPD-02.IIIa-A2	P02.5	411	482	15	1	10	11	11	33	11
P02	LPD-02.IIIb-A2	P02.6	0	0	0	0	0	0	0	0	0
P02	LPD-02.IIIb-A2	P02.7	221	261	9	1	5	6	6	18	6
P02	LPD-02.IIIb-A2	P02.8	0	0	0	0	0	0	0	0	0
P01	LPD-01.I-A2	P01.1	357	407	7	1	8	9	9	27	9
P01	LPD-01.I-A2	P01.2	0	0	0	0	0	0	0	0	0
P01	LPD-01.II-A2	P01.3	188	231	12	0	5	5	5	15	5
P01	LPD-01.II-A2	P01.4	0	0	0	0	0	0	0	0	0
P01	LPD-01.IIIa-A2	P01.5	147	184	11	0	4	4	4	12	4
P01	LPD-01.IIIa-A2	P01.6	0	0	0	0	0	0	0	0	0
P01	LPD-01.IIIb-A2	P01.7	368	431	13	0	9	9	9	27	9
P01	LPD-01.IIIb-A2	P01.8	0	0	0	0	0	0	0	0	0
P00	LPD-00.I-A2	P00.1	164	200	10	1	4	5	5	15	5
P00	LPD-00.I-A2	P00.2	0	0	0	0	0	0	0	0	0
P00	LPD-00.IIa-A2	P00.3	379	471	27	0	10	10	10	30	10
P00	LPD-00.IIa-A2	P00.4	0	0	0	0	0	0	0	0	0
P00	LPD-00.IIb-A2	P00.5	837	975	27	1	20	21	21	63	21
P00	LPD-00.IIb-A2	P00.6	0	0	0	0	0	0	0	0	0
P00	LPD-00.IIIa-A2	P00.7	316	372	12	0	8	8	8	24	8
P00	LPD-00.IIIa-A2	P00.8	0	0	0	0	0	0	0	0	0
P00	LPD-00.IIIb-A2	P00.9	201	239	9	0	5	5	5	15	5
P00	LPD-00.IIIb-A2	P00.10	0	0	0	0	0	0	0	0	0
P1	LPD-1.I-A2	P1.1	113	142	9	0	3	3	3	9	3
P1	LPD-1.I-A2	P1.2	0	0	0	0	0	0	0	0	0
P1	LPD-1.II-A2	P1.3	534	633	23	1	13	14	14	42	14
P1	LPD-1.II-A2	P1.4	0	0	0	0	0	0	0	0	0
P1	LPD-1.IIIa-A2	P1.5	463	535	13	1	11	12	12	36	12

P1	LPD-1.IIIb-A2	P1.6	0	0	0	0	0	0	0	0	0
P1	LPD-1.IIIb-A2	P1.7	435	505	13	0	11	11	11	33	11
P1	LPD-1.IIIb-A2	P1.8	0	0	0	0	0	0	0	0	0
P01	BPD-A1	P01.5	0	0	0	0	0	0	0	0	0
P01	BPD-A1	P01.6	0	0	0	0	0	0	0	0	0
P01	BPD-A1	P01.7	0	0	0	0	0	0	0	0	0
P01	LPD-01.II-A1	P01.3	0	0	0	0	0	0	0	0	0
P01	LPD-01.II-A1	P01.4	0	0	0	0	0	0	0	0	0
P01	LPD-01.I-A1	P01.1	0	0	0	0	0	0	0	0	0
P01	LPD-01.I-A1	P01.2	0	0	0	0	0	0	0	0	0
P00	LPD-00.I-A1	P00.1	318	380	15	0	8	8	8	24	8
P00	LPD-00.I-A1	P00.2	0	0	0	0	0	0	0	0	0
P3	LPD-3.I-A1	P3.1	281	349	20	1	7	8	8	24	8
P3	LPD-3.I-A1	P3.2	0	0	0	0	0	0	0	0	0
P6	LPD-6.I-A1	P6.1	0	0	0	0	0	0	0	0	0
P6	LPD-6.I-A1	P6.2	0	0	0	0	0	0	0	0	0
P7	LPD-7.I-A1	P7.1	0	0	0	0	0	0	0	0	0
P7	LPD-7.I-A1	P7.2	0	0	0	0	0	0	0	0	0
P10	LPD-10.I-A1	P10.1	0	0	0	0	0	0	0	0	0
P10	LPD-10.I-A1	P10.2	0	0	0	0	0	0	0	0	0
P11	LPD-11.II-A1	P11.1	0	0	0	0	0	0	0	0	0
P11	LPD-11.II-A1	P11.2	0	0	0	0	0	0	0	0	0
P11	LPD-11.III-A1	P11.3	0	0	0	0	0	0	0	0	0
P11	LPD-11.III-A1	P11.4	0	0	0	0	0	0	0	0	0
P12	LPD-12.I-A1	P12.1	0	0	0	0	0	0	0	0	0
P12	LPD-12.I-A1	P12.2	0	0	0	0	0	0	0	0	0
P13	LPD-13.I-A1	P13.1	0	0	0	0	0	0	0	0	0
P13	LPD-13.I-A1	P13.2	0	0	0	0	0	0	0	0	0
P16	LPD-16.II-A1	P16.1	0	0	0	0	0	0	0	0	0
P16	LPD-16.II-A1	P16.2	0	0	0	0	0	0	0	0	0
P16	LPD-16.II-A1	P16.3	0	0	0	0	0	0	0	0	0
P16	LPD-16.II-A1	P16.4	0	0	0	0	0	0	0	0	0
P16	LPD-16.III-A1	P16.5	0	0	0	0	0	0	0	0	0
P16	LPD-16.III-A1	P16.6	0	0	0	0	0	0	0	0	0
P16	LPD-16.III-A1	P16.7	0	0	0	0	0	0	0	0	0
P16	LPD-16.III-A1	P16.8	0	0	0	0	0	0	0	0	0
P17	LPD-17.I-A1	P17.1	0	0	0	0	0	0	0	0	0
P17	LPD-17.I-A1	P17.2	0	0	0	0	0	0	0	0	0
P17	LPD-17.I-A1	P17.3	0	0	0	0	0	0	0	0	0
P17	LPD-17.I-A1	P17.4	0	0	0	0	0	0	0	0	0

systemy CCTV, SKD, SSWiN, przyzywowa

poziom	Nazwa PD	nazwa szafy	kamery	kontrolery KD i SSWiN	przyzywowa	suma portów (z uwzgl. zapasu)			panel 48xRJ45	wieszak 1U	wypełnienie szaf [U]	kable stakujące
							24	48				
P02	BPD-A2	BPD.1	0	0	0	0	0	0	0	0	0	0
P02	BPD-A2	BPD.2	6	1	0	8	1	0	1	1	3	0
P02	BPD-A2	BPD.3	0	0	0	0	0	0	0	0	0	0
P02	BPD-A2	BPD.4	0	0	0	0	0	0	0	0	0	0
P02	BPD-A2	BPD.5	0	0	0	0	0	0	0	0	0	0
P02	LPD-02.I-A2	P02.1	0	0	0	0	0	0	0	0	0	0
P02	LPD-02.I-A2	P02.2	1	1	2	4	1	0	1	1	3	0
P02	LPD-02.II-A2	P02.3	0	0	0	0	0	0	0	0	0	0
P02	LPD-02.II-A2	P02.4	11	1	1	14	1	0	1	1	3	0
P02	LPD-02.IIIa-A2	P02.5	0	0	0	0	0	0	0	0	0	0
P02	LPD-02.IIIb-A2	P02.6	0	1	2	3	1	0	1	1	3	0
P02	LPD-02.IIIb-A2	P02.7	0	0	0	0	0	0	0	0	0	0
P02	LPD-02.IIIb-A2	P02.8	4	1	2	8	1	0	1	1	3	0
P01	LPD-01.I-A2	P01.1	0	0	0	0	0	0	0	0	0	0
P01	LPD-01.I-A2	P01.2	12	1	2	17	1	0	1	1	3	0
P01	LPD-01.II-A2	P01.3	0	0	0	0	0	0	0	0	0	0
P01	LPD-01.II-A2	P01.4	2	1	2	6	1	0	1	1	3	0
P01	LPD-01.IIIa-A2	P01.5	0	0	0	0	0	0	0	0	0	0
P01	LPD-01.IIIa-A2	P01.6	9	1	1	12	1	0	1	1	3	0
P01	LPD-01.IIIb-A2	P01.7	0	0	0	0	0	0	0	0	0	0
P01	LPD-01.IIIb-A2	P01.8	13	1	3	19	1	0	1	1	3	0
P00	LPD-00.I-A2	P00.1	0	0	0	0	0	0	0	0	0	0
P00	LPD-00.I-A2	P00.2	2	1	3	7	1	0	1	1	3	0
P00	LPD-00.IIa-A2	P00.3	0	0	0	0	0	0	0	0	0	0
P00	LPD-00.IIa-A2	P00.4	16	2	4	24	1	0	1	1	3	0
P00	LPD-00.IIb-A2	P00.5	0	0	0	0	0	0	0	0	0	0
P00	LPD-00.IIb-A2	P00.6	21	1	3	28	2	0	1	1	4	2
P00	LPD-00.IIIa-A2	P00.7	0	0	0	0	0	0	0	0	0	0
P00	LPD-00.IIIa-A2	P00.8	3	1	3	8	1	0	1	1	3	0
P00	LPD-00.IIIb-A2	P00.9	0	0	0	0	0	0	0	0	0	0
P00	LPD-00.IIIb-A2	P00.10	14	1	2	19	1	0	1	1	3	0
P1	LPD-1.I-A2	P1.1	0	0	0	0	0	0	0	0	0	0
P1	LPD-1.I-A2	P1.2	0	1	3	4	1	0	1	1	3	0

P1	LPD-1.II-A2	P1.3	0	0	0	0	0	0	0	0	0	0
P1	LPD-1.II-A2	P1.4	1	1	3	6	1	0	1	1	3	0
P1	LPD-1.IIIa-A2	P1.5	0	0	0	0	0	0	0	0	0	0
P1	LPD-1.IIIb-A2	P1.6	1	1	0	2	1	0	1	1	3	0
P1	LPD-1.IIIb-A2	P1.7	0	0	0	0	0	0	0	0	0	0
P1	LPD-1.IIIb-A2	P1.8	4	1	0	6	1	0	1	1	3	0
P01	BPD-A1	P01.5	0	0	0	0	0	0	0	0	0	0
P01	BPD-A1	P01.6	0	1	0	1	0	0	1	1	2	0
P01	BPD-A1	P01.7	0	0	0	0	0	0	0	0	0	0
P01	LPD-01.II-A1	P01.3	0	0	0	0	0	0	0	0	0	0
P01	LPD-01.II-A1	P01.4	0	0	0	0	0	0	0	0	0	0
P01	LPD-01.I-A1	P01.1	0	0	0	0	0	0	0	0	0	0
P01	LPD-01.I-A1	P01.2	0	0	0	0	0	0	0	0	0	0
P00	LPD-00.I-A1	P00.1	0	0	0	0	0	0	0	0	0	0
P00	LPD-00.I-A1	P00.2	8	0	4	13	1	0	1	1	3	0
P3	LPD-3.I-A1	P3.1	0	0	0	0	0	0	0	0	0	0
P3	LPD-3.I-A1	P3.2	7	0	3	11	1	0	1	1	3	0
P6	LPD-6.I-A1	P6.1	0	0	0	0	0	0	0	0	0	0
P6	LPD-6.I-A1	P6.2	0	0	0	0	0	0	0	0	0	0
P7	LPD-7.I-A1	P7.1	0	0	0	0	0	0	0	0	0	0
P7	LPD-7.I-A1	P7.2	0	0	0	0	0	0	0	0	0	0
P10	LPD-10.I-A1	P10.1	0	0	0	0	0	0	0	0	0	0
P10	LPD-10.I-A1	P10.2	0	0	0	0	0	0	0	0	0	0
P11	LPD-11.II-A1	P11.1	0	0	0	0	0	0	0	0	0	0
P11	LPD-11.II-A1	P11.2	0	0	0	0	0	0	0	0	0	0
P11	LPD-11.III-A1	P11.3	0	0	0	0	0	0	0	0	0	0
P11	LPD-11.III-A1	P11.4	0	0	0	0	0	0	0	0	0	0
P12	LPD-12.I-A1	P12.1	0	0	0	0	0	0	0	0	0	0
P12	LPD-12.I-A1	P12.2	0	0	0	0	0	0	0	0	0	0
P13	LPD-13.I-A1	P13.1	0	0	0	0	0	0	0	0	0	0
P13	LPD-13.I-A1	P13.2	0	0	0	0	0	0	0	0	0	0
P16	LPD-16.II-A1	P16.1	0	0	0	0	0	0	0	0	0	0
P16	LPD-16.II-A1	P16.2	0	0	0	0	0	0	0	0	0	0
P16	LPD-16.II-A1	P16.3	0	0	0	0	0	0	0	0	0	0
P16	LPD-16.II-A1	P16.4	0	0	0	0	0	0	0	0	0	0
P16	LPD-16.III-A1	P16.5	0	0	0	0	0	0	0	0	0	0
P16	LPD-16.III-A1	P16.6	0	0	0	0	0	0	0	0	0	0
P16	LPD-16.III-A1	P16.7	0	0	0	0	0	0	0	0	0	0

P16	LPD-16.III-A1	P16.8	0	0	0	0	0	0	0	0	0	0
P17	LPD-17.I-A1	P17.1	0	0	0	0	0	0	0	0	0	0
P17	LPD-17.I-A1	P17.2	0	0	0	0	0	0	0	0	0	0
P17	LPD-17.I-A1	P17.3	0	0	0	0	0	0	0	0	0	0
P17	LPD-17.I-A1	P17.4	0	0	0	0	0	0	0	0	0	0

Na szaro zaznaczono obszary wyłączone z zakresu niniejszego opracowania, które będą ewentualnie realizowane w kolejnych etapach inwestycji.

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, jak i jeden spójny system kontroli dostępu do sieci LAN. Jednocześnie spójność zastosowanych rozwiązań, zapewnia elastyczność w czasie utrzymania i rozbudowy poszczególnych węzłów sieci LAN, jak i odpowiednich komponentów do zarządzania infrastrukturą sieciową.

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)
BPD-A2	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	4	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 3 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	20	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
	Przełącznik szkieletowy LAN: 48x10GBASE-X SFP+, 6x40GBASE-X QSFP+/2xQSFP28	2	46 x 10GBase-LR, SFP+, 2 x 10GBase-	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 40GBASE QSFP+ (kabel passive

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
			SR, 2 x 40GBASE passive cable 1m, 38 x 1GBase-LX 2 x 40G passive cable 5m, do podłączenia z warstwą serwerową – przełącznikami, 2 x 40G QSFP+ LC do podłączenia z budynkiem A1	copper: 2x 1m). Możliwość rozbudowy stosu o kolejne przełączniki sieciowe. Zasilacze redundante per przełącznik sieciowy. Redundante wentylatory.
	Przełącznik serwerowy LAN: 48x1/10GBASE-T, 6xQSFP+/2xQSFP28	2	2 x 40G QSFP+ 1 m DAC, 2x40GBase passive cabel 5 m,	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 40GBASE QSFP+ (kabel passive copper: 2x 5m). Możliwość rozbudowy stosu o kolejne przełączniki sieciowe. Zasilacze redundante per przełącznik sieciowy. Redundante wentylatory
	System do zarządzania infrastrukturą LAN	1	Do 200 urządzeń węzłów sieci LAN	Pracujące na serwerze przedstawionym poniżej, **w postaci maszyny wirtualnej**, na maszynie wirtualnej
	System NAC – wersja zaawansowana	1	Do 5k urządzeń końcowych jednocześnie zarządzanych	System uruchomiony na serwerze, **w postaci maszyny wirtualnej** na serwerze
	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	System do wirtualizacji zasobów pozwalający na uruchomienie maszyn wirtualnych z poszczególnymi aplikacjami i systemami, jak powyżej

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
			przełączników serwerowych ToR	
	Firewall typu NGFW, z zapewnieniem wirtualnych kontekstów, w celu separacji elementów bezpieczeństwa, zgodnie z wymaganiami	2	4 x 10GBASE-X SFP+, moduły 4 x 10GBase-T	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, 2 x E1	System do realizacji funkcjonalności komunikacji pomiędzy szpitalem i systemami zewnętrznymi telefonicznymi, w oparciu o połączenia cyfrowe ISDN
LPD-02.I-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	1	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-02.II-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 4 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	3		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	30	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)
LPD-02.IIIa-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie dwóch stosów przełączników sieciowych, w oparciu o dedykowane połączenia 11 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	10		
	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.
LPD-02.IIIb-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	5		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	2	2 x 2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN. Stworzenie stosu przełączników w oparciu o 2 x kabel 1 x10G passive copper DAC
	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.
LPD-01.I-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 9 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	8		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	7	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)
LPD-01.II-A2	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	5	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	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.
LPD-01.IIIa-A2	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	4	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 4 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	11	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-01.IIIb-A2	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	9	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 9 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
			A2	
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	13	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-00.I-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	4		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	10	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-00.IIa-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie dwóch stosów przełączników sieciowych, w oparciu o dedykowane połączenia 10 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	9		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	27	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-00.IIb-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	3 x 2 x 10GBase-LR – połączenie do warstwy szkieletowej	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN.

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	20	LAN w budynku A2	Stworzenie trzech stosów przełączników sieciowych, w oparciu o dedykowane połączenia 21 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	2	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN. Stworzenie stosu przełączników w oparciu o 1x10GBASE SFP+) kabel passive copper).
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	27	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-00.IIIa-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie dwóch stosów przełączników sieciowych, w oparciu o dedykowane połączenia 8 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	7		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	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.
LPD-01.IIIb-A2	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	5	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 5 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
	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.
LPD-1.I-A2	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	3	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 3 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	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.
LPD-00.IIb-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie dwóch stosów przełączników sieciowych, w oparciu o dedykowane połączenia 14 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	13		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN.
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	23	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-1.IIIa-A2	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie dwóch stosów przełączników sieciowych, w oparciu o dedykowane połączenia 12 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	11		

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN.
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	13	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-1.IIIb-A2	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	11	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie dwóch stosów przełączników sieciowych, w oparciu o dedykowane połączenia 11 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	13	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
BPD-A1	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN
	Przełącznik szkieletowy LAN: 24x10GBASE-X SFP+, 6x40GBASE-X QSFP+/2xQSFP28	2	4 x 10GBase-LR SFP+ 2 x 40GBASE passive cable 1m, 6 x 1GBase-LX, 2 x 40G passive cable 5m, do podłączenia z warstwą serwerową – przełącznikami, 2 x 40G QSFP+ LC do podłączenia z budynkiem A2	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 40GBASE QSFP+ (kabel passive copper: 2x 1m). Możliwość rozbudowy stosu o kolejne przełączniki sieciowe. Zasilacze redundante per przełącznik sieciowy. Redundante wentylatory.

Nazwa punktu dystrybucyjnego	Typ/model urządzenia	Ilość	Liczba obsadzonych połączeń sieciowych – typu uplink	Inne wymagania (ogólnie)
	Przełącznik serwerowy LAN: 48x1/10GBASE-T, 6xQSFP+/2xQSFP28	2	2 x 40G QSFP+ 1 m DAC, 2x40GBase passive cabel 5 m,	Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 2 x 40GBASE QSFP+ (kabel passive copper: 2x 5m). Możliwość rozbudowy stosu o kolejne przełączniki sieciowe. Zasilacze redundante per przełącznik sieciowy. Redundante wentylatory
LPD-00.I-A1	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 8 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	7		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN.
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	16	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.
LPD-3.I-A1	Przełącznik LAN: 24x10/100/1000BASE-T, 4x10GBASE-X SFP+	1	2 x 10GBase-LR – połączenie do warstwy szkieletowej LAN w budynku A2	Wspólna architektura systemu, jak w pozostałych węzłach sieci – ten sam rodzaj przełączników sieci LAN. Stworzenie stosu przełączników sieciowych, w oparciu o dedykowane połączenia 8 x 10GBASE SFP+ (kabel passive copper). Wszystkie porty SFP+ aktywne i możliwe do wykorzystania.
	Przełącznik LAN: 48x10/100/1000BASE-T POE+, 4x10GBASE-X SFP+	7		
	Przełacznik Security: 24 porty 1000Base-X, PoE+, 4 x 10/100/100 combo, 4x1GBASE-X SFP	1	2 x 1GBase-LX – połączenie do warstwy szkieletowej w budynku A2	Spójna konfiguracja i polityka dostępu per przełącznik w sieci LAN, w odniesieniu do pozostałych węzłów sieci LAN.
	Access Point – dostęp do sieci bezprzewodowej, zgodnie ze standardem 802.11b/g/n/ac wave 2	16	Połączenie typu UTP	Zasilanie poprzez PoE. Centralnie zarządzane z poziomu dedykowanego kontrolera sieci bezprzewodowej.

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 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.

Wymagania szczegółowe dla systemu zarządzania siecią LAN

Wymagania, realizowane w ramach projektowane systemu zarządzania infrastruktura sieciową, jej poszczególnymi komponentami sieci LAN:

1. System musi być zbudowany w architekturze klient – serwer
2. Dostęp do sytemu zarządzania musi być realizowany przez przeglądarkę internetową
3. System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność
4. System zarządzania musi spełniać podstawowe funkcje:
    a. Automatyczne wykrywaine topologii sieci,
    b. Monitorowanie stanu urządzeń po protokole SNMP,
    c. Konfiguracja urządzeń po protokole SNMP,

d. Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach,

e. Konfiguracja VLANów na zarządzanych urządzeniach,

f. Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania,

g. Zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń

h. Możliwość wysyłania alarmów np. mailem lub SMS'em,

i. Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta,

j. Obrazowanie sieci w postaci mapki wraz z wyróżnianiem kolorami występujących alarmów,

k. Lokalizowanie użytkowników po adresie IP lub MAC,

l. Możliwość utworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym.

5. Muszą być dostępne moduły umożliwiające rozbudowę i integrację systemu o następujące funkcjonalności:

a. Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA,

b. Obługa informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników,

c. Zarządzenie systemem telefonii IP,

d. Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS,

e. Moduł do monitorowania stanu/zdrowia usług.

6. Niezbędne jest aby system zarządzania był w stanie podłączyć się i importować dane z Active Directory – jeżeli będzie dostarczony przez Szpital.

7. System musi mieć możliwość automatycznego tworzenia i rozsyłania raportów.

8. Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń.

9. System musi wspierać co najmniej 200 urządzeń w ramach standardowo dostarczanego sytemu, w tym różnych producentów urządzeń sieciowych.

10. Dla wszystkich obsługiwanych standardowo urządzeń musi być dostępnie nie tylko monitorowanie ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń.

11. Musi również mieć możliwość implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów.

Wymagania szczegółowe dla kompleksowego systemu kontroli dostępu do sieci

System kontroli dostępu do sieci LAN, w pełni zintegrowany w zakresie zaprojektowanych urządzeń/przełączników, 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. 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.

1. System kontroli dostępu musi być dostępny w postaci maszyny wirtualnej dostępnej na systemie wirtualnym VMWare. System kontroli dostępu musi się składać z aplikacji zarządzającej pozwalającej na konfigurację systemu kontroli dostępu do sieci oraz serwerów RADIUS, które zapewniają uwierzytelnianie oraz autoryzację dostępu do sieci. Wymaga się, aby pojedynczy system kontroli dostępu był w stanie obsłużyć do minimum 5000 systemów końcowych.

2. System powinien być posiadać licencję umożliwiającą obsłużenie do min. 5000 systemów końcowych.

3. System kontroli dostępu musi zapewniać możliwość uwierzytelniania użytkowników (Proxy) do innych systemów uwierzytelniających RADIUS, LDAP/Microsoft Active Directory oraz lokalnej bazy użytkowników. Musi istnieć możliwość wyboru systemu uwierzytelniającego na podstawie:

   a. Typu uwierzytelnienia np. IEEE 802.1x, MAC authentication (PAP, CHAP, MsCHAP, EAP- MD5), dostęp do zarządzania urządzeń itp.

   b. Nazwy użytkownika, MAC adresu lub nazwy Host urządzenia.

4. Po przeprowadzeniu uwierzytelnienia musi następować autoryzacja dostępu do sieci. Wybór konkretnej autoryzacji dostępu musi być możliwy na podstawie następujących parametrów:

   a. Typu uwierzytelniania np. IEEE 802.1x, MAC authentication, Management Authentication wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MsCHAP), MAC (MD5) itp.

   b. Grupy użytkowników bazujące na grupach LDAP/Microsoft Active Directory, grupach RADIUS lub grupach nazw użytkowników wpisanych ręcznie.

   c. Systemów końcowych bazujących na nazwie systemu końcowego (Hostname), adresie IP, przynależności systemu końcowego do grupy LDAP/Microsoft Active Directory, MAC adresie.

   d. Typów urządzeń końcowych np. Android, iOS, Mac, Linux, Windows Mobile itp.

   e. Lokalizacji - np. adresy IP przełączników, które przeprowadzają autoryzację wraz z możliwością wskazania konkretnych portów.

   f. Czasu - np. codziennie pomiędzy godziną 9:00 a 17:00.

5. Aplikacja powinna posiadać możliwość tworzenia Profili autoryzacyjnych, które określają biznesową rolę użytkownika w sieci np.: Administrator, Księgowość, Radcy Prawni, Goście, Studenci, Pracownicy itp. Rola taka powinna być powiązana z polityką jaką

będziemy chcieli wymusić na urządzeniach klienckich (przełącznikach, sieci bezprzewodowej itp.).

6. Profil autoryzacyjny powinien wskazywać na Politykę, jaka musi zostać wysłana do urządzenia aby zapewnić właściwą autoryzację dostępu systemu końcowego do sieci.

7. Polityka musi zapewniać możliwość wysłania standardowych atrybutów RADIUS w ramach których będzie możliwe ustawienie: sieci VLAN do której użytkownika ma mieć dostęp, listy kontroli dostępu ACL oraz Quality of Service. Ponieważ oprócz przydziału sieci VLAN różne urządzenia mogą wymagać wysłania różnych atrybutów istnieje konieczność zapewnienia możliwości definiowania wysyłanych atrybutów dla każdego urządzenia z osobna. Przykładowo dla większości przełączników przydzielenie systemu końcowego do sieci VLAN wymaga wysłania następujących atrybutów: Tunnel-Type, Tunnel-Medium-Type oraz Tunnel-Private-Group-ID. Ten ostatni atrybut zawiera faktycznie wymagany VLAN ID lub nazwę VLAN. Niektóre urządzenia posiadają własne atrybuty VSA (Vendor Specyfic Attributes). Polityka musi zapewniać możliwość wysyłania atrybutów VSA dla uzyskania odpowiedniej autoryzacji systemu końcowego w sieci.

8. System kontroli dostępu musi zapewniać wsparcie dla wymuszenia zmiany autoryzacji CoA (Change of Authorization) zgodnie z RFC 3576 oraz RFC 5176. Ze względu na różną implementację powyższych RFC na różnych urządzeniach sieciowych wymaga się, aby istniała możliwość konfiguracji portu oraz formatu MAC adresu wysyłanego do urządzenia sieciowego w przypadku wymuszenia zmiany autoryzacji.

9. System kontroli dostępu musi zapewniać wsparcie dla wymuszenia zmiany autoryzacji z wykorzystaniem protokołu SNMP - rozwiązanie stosowane przez niektórych producentów sprzętu sieciowego.

10. System kontroli dostępu musi zapewniać wsparcie dla wymuszenia zmiany autoryzacji poprzez wyłączenie i włączenie portu.

11. System kontroli dostępu musi zapewnić interfejs konfiguracyjny pracujący w architekturze klient/serwer. Preferowane jest rozwiązanie korzystające z przeglądarki www.

12. System kontroli dostępu musi zapewniać bieżącą widzialność dopuszczonych do sieci systemów końcowych. Wymaga się, aby widziane były następujące parametry systemu końcowego i jego stanu:

a. MAC adres systemu końcowego,

b. Adres IP systemu końcowego,

c. Nazwa komputera - Host Name,

d. Typ systemu końcowego oraz system operacyjny - możliwość wykrywania urządzeń na podstawie zapytań DHCP (DHCP fingerprinting) np. Windows/ Windows 2012, iPhone / Android itp.,

e. Nazwa urządzenia, do którego dołączony jest klient - to może być nazwa kontrolera bezprzewodowego lub nazwa przełącznika sieciowego,

f. Adres IP urządzenia, do którego dołączony jest klient i które przeprowadza uwierzytelnienie i autoryzację systemu końcowego,

g. Typ uwierzytelniania systemu końcowego np. MAC authentication, IEEE 802.1x wraz z informacją o wykorzystywanym protokole EAP np. PEAP, EAP-MD5, EAP-TLS itp.

13. System kontroli dostępu musi zapewniać przechowywanie historii dostępu systemu końcowego do sieci.

14. System kontroli dostępu musi zapewniać możliwość wymuszenia ponownej autoryzacji wskazanego systemu końcowego z wykorzystaniem wymaganych powyżej funkcjonalności CoA.

15. System kontroli dostępu musi zapewniać możliwość szybkiego przeniesienia wskazanego systemu do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci tzw. grupa Black List.

16. System kontroli dostępu musi umożliwiać uruchomienie systemu kontroli dostępu do sieci poprzez stronę www tzw. Captive Portal. Captive Portal powinien zapewniać:

    a. Możliwość logowania do sieci klientów, którzy nie posiadają suplikanta IEEE 802.1x wraz z możliwością zapamiętania tego systemu na wskazany czas tak, aby nie trzeba było za każdym razem ponownie wprowadzać nazwy użytkownika i hasła na stronie www.

    b. Konieczność akceptację regulaminu przed wpuszczeniem systemu końcowego do sieci.

    c. Możliwość rejestracji systemu końcowego z wymaganiem wprowadzenia przez użytkownika wymaganych danych np. imię, nazwisko, numer telefonu, adres e-mail i inne pola definiowane przez administratora.

    d. Możliwość wpuszczania systemu końcowego do sieci po rejestracji systemu końcowego oraz wymaganej akceptacji dostępu przez tzw. sponsora, który musi zaakceptować dostęp dla zarejestrowanego gościa.

17. System kontroli dostępu musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa.

18. Agent musi być dostępny min. na systemy operacyjne Windows oraz MAC OS.

19. System musi zapewniać współpracę z systemami MDM (Mobile Device Management) w celu sprawdzania zgodności z polityką bezpieczeństwa dla urządzeń mobilnych.

20. System kontroli dostępu powinien posiadać interfejs API pozwalający na prostą integrację systemu kontroli dostępu z systemami 3rd party.

21. System musi posiadać funkcję OnBoard z funkcją wystawiania certyfikatów zaufanych dla poszczególnych ilości urządzeń, w ramach licencji głównej. System musi posiadać funkcję automatycznej rejestracji urządzeń oraz samodzielne zarządzanie cyklem ich życia przez samoobsługowy portal dostępny dla pracowników po podaniu korporacyjnych danych uwierzytelniających. Widok portalu w sposób automatyczny powinien dopasowywać się do rozmiaru ekranu urządzenia mobilnego. Administratorzy muszą mieć możliwość przygotowywania własnego portalu korzystając z wbudowanych szablonów.

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

Kontroler sieci bezprzewodowej w momencie dostawy musi obsługiwać minimum 300 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.

Kontroler sieci WLAN musi być dostarczony jako maszyna wirtualna, musi wspierać środowisko co najmniej VMware ESXi.

Mechanizmy przekazywania danych

Kontroler musi obsługiwać jednocześnie różne mechanizmy przekazywania danych, w tym routing, tunelowanie ruchu z AP (Bridge@Controller) i zamykanie ruchu w AP (Bridge@AP).

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).

Zarządzanie

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.

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 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

1. RAID 5 w oparciu o dedykowany kontroler.

Dyski twarde

1. 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

1. 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 – 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 i ilościami portów zostały uwzględnione poniżej w specyfikacji.

1. Minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T wspierające standard 802.3at (PoE+).
2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).
3. Przepustowość: minimum 176 Gb/s.
4. Wydajność: minimum 130 Mp/s.
5. Wysokość w szafie 19” – 1U, głębokość nie większa niż 36 cm.
6. Tablica adresów MAC o wielkości minimum 16k pozycji.
7. Budżet mocy dla PoE minimum 370W.
8. Obsługa ramek Jumbo.
9. Możliwość łączenia urządzeń w stosy (minimum 9 urządzeń w stosie, urządzenia połączone w stos widziane jako jedno logiczne urządzenie) z wykorzystaniem portów 10Gb/s.
10. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP.
11. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng.
12. Minimum 32 interfejsy IP VLAN.
13. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping.

14. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol.

15. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN.

16. Obsługa IEEE 802.1ad QinQ i Selective QinQ.

17. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree.

18. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom.

19. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6).

20. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.

21. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia

22. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu).

23. Obsługa standardu 802.1p – min. 8 kolejek na porcie.

24. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p.

25. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP.

26. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ogranicznia pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s.

27. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring.

28. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

• Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x,

• Możliwość uwierzytelniania wielu użytkowników na jednym porcie,

• Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS,

• Przypisanie profilu QoS dla użytkownika lub grupy użytkowników.

29. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED.

30. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC.

31. TACACS+ i RADIUS Network Login.

32. RADIUS Accounting.

33. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS.

34. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https.

35. Syslog.

36. NTP.

37. Obsługa protokołów 802.3ah oraz 802.1ag.

38. Możliwość przechowywania wielu wersji oprogramowania na przełączniku.

39. Możliwość przechowywania wielu plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej.

40. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego.

41. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol.

42. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych.

43. Minimalny zakres pracy od -5°C do 45°C.

44. Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający dostarczenie sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego.

45. Przełącznik powinien pochodzić z oficjalnego kanału dystrybucji producenta.

46. Przełącznik musi być fabrycznie nowy.

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:

1. Minimum 24 porty 10BASE-T/100BASE-TX/1000BASE-T wspierające standard 802.3at (PoE+) na potrzeby podłączenia urządzeń Security, jak CCTV itp.

2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP) obsadzone odpowiednio w zależności od rodzaju systemu LAN/Security.

3. Przepustowość: minimum 128 Gb/s.

4. Wydajność: minimum 95 Mp/s.

5. Wysokość w szafie 19” – 1U, głębokość nie większa niż 30 cm.

6. Tablica adresów MAC o wielkości minimum 16k pozycji.

7. Budżet mocy dla PoE minimum 370W.

8. Obsługa ramek Jumbo.

9. Możliwość łączenia urządzeń w stosy (minimum 9 urządzeń w stosie, urządzenia połączone w stos widziane jako jedno logiczne urządzenie) z wykorzystaniem portów 10Gb/s.

10. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP.

11. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng.

12. Minimum 32 interfejsy IP VLAN.

13. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping.

14. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol.

15. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN.

16. Obsługa IEEE 802.1ad QinQ i Selective QinQ.

17. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree.

18. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom.

19. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6).

20. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.

21. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia.

22. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu).

23. Obsługa standardu 802.1p – min. 8 kolejek na porcie.

24. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p.

25. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP.

26. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ogranicznia pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s.

27. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring.

28. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

• Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x,

• Możliwość uwierzytelniania wielu użytkowników na jednym porcie,

• Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS,

• Przypisanie profilu QoS dla użytkownika lub grupy użytkowników.

29. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED.

30. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC.

31. TACACS+ i RADIUS Network Login.

32. RADIUS Accounting.

33. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS

34. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https.

35. Syslog.

36. NTP.

37. Obsługa protokołów 802.3ah oraz 802.1ag.

38. Możliwość przechowywania wielu wersji oprogramowania na przełączniku.

39. Możliwość przechowywania wielu plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej.

40. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego.

41. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol.

42. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych.

43. Minimalny zakres pracy od -5°C do 45°C.

44. Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający dostarczenie sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego.

45. Przełącznik powinien pochodzić z oficjalnego kanału dystrybucji producenta.

46. Przełącznik musi być fabrycznie nowy.

Przełącznik spine/warstwa szkieletowa sieci LAN – 48 portów 1/10GBASE-X SFP+, 6 x 40G BASE-X QSFP+/2QSFP28

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.

1. Typ i liczba portów:

• Minimum 48 porty 1/10GBase-X, SFP+,

• Minimum 6 porty 40GbE QSFP+/2 porty QSFP28.

2. Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management.

3. Port konsoli RS232 ze złączem DB9 lub RJ45.

4. Port USB 2.0.

5. Przepustowość minimum 1071 Mp/s dla pakietów 64 bajtowych, przy zachowaniu opóźnienia dla 10G nie mniejszego niż 1.5s.

6. Wydajność: minimum 1440 Gb/s (prędkość przełączania „wirespeed" dla każdego portu przełącznika),

7. Przełączanie w warstwie 2 i 3 modelu OSI.

8. Wielkość bufora pakietów (packet buffer): minimum 12MB.

9. Minimum 1G pamięci typu Flash.

10. Minimum 4GB pamięci operacyjnej.

11. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów).

12. Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza.

13. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.

14. Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie ze wspólnym zarządzaniem. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 320 portów 10GbE SFP+. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)).

15. Łączenie w stos z wykorzystaniem portów 10Gb, 40Gb i agregowanych portów 10Gb (w celu zwiększenia przepustowości w stosie).

16. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie

17. Tablica adresów MAC o wielkości minimum 208K pozycji.

18. Obsługa ramek Jumbo.

19. Obsługa Quality of Service.

20. Obsługa mechanizmów: strict priority (SP) queuing, weighted fair queuing (WFQ), weighted random early discard (WRED), SP+WFQ .

21. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol.

22. Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ.

23. Obsługa IGMP v1/v2/v3, IGMP Snooping v1/v2/v3, PIM DM, PIM SM, MLD snooping v1/v2 oraz IPv6 PIM Snooping.

24. Wsparcie dla FibreChannel over Ethernet (FCF/Transit/NPV).

25. Wsparcie dla Data Center Bridging (DCB):

• IEEE 802.1Qbb Priority Flow Control (PFC)

• Data Center Bridging Exchange (DCBX)

26. Routing IPv4 – statyczny i dynamiczny (min. RIP, IS-IS, OSPF, BGP).

27. Routing IPv6 – statyczny i dynamiczny (min. RIPng, IS-ISv6, OSPFv3).

28. Obsługa ECMP (Equal Cost Multi Path) .

29. Tablica routingu o pojemności co najmniej 16K wpisów.

30. Serwer DHCP, klient DHCP, obsługa opcji 82 (snooping i relay), DHCP Snooping.

31. Obsługa list ACL na bazie informacji z warstw 3/4 modelu OSI.

Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia

32. Obsługa standardu 802.1p.

33. Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p.

34. Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, remote mirroring

35. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x.

36. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS.

37. Zarządzanie poprzez port konsoli, SNMP v.1, 2c i 3, Telnet, SSH v.2.

38. Syslog.

39. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED.

40. Obsługa sFlow.

41. Obsługa NETCONF.

42. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3.

43. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter.

44. Obsługa Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) oraz kompatybilność z Precision Time Protocol (PTP) RFC 1855.

45. Obsługa OAM (IEEE 802.3ah).

46. Obsługa CFD (IEEE 802.1ag).

47. Modularny system operacyjny ze wsparciem dla In Services Software Upgrade (ISSU) i skryptów w języku Python.

48. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).

49. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).

50. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

51. Wysokość w szafie 19" – 1U.

52. Maksymalny pobór mocy nie większy niż 450W

53. Minimalny zakres temperatur pracy od 0°C do 40°C.

54. Minimum 5 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na wymianę na maksymalnie następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika (co najmniej 10 lat), również po wygaśnięciu kontraktu serwisowego.

55. Przełącznik powinien pochodzić z oficjalnego kanału dystrybucji producenta.

56. Przełącznik musi być fabrycznie nowy.

Przełącznik do warstwy serwerowej sieci LAN – 48 portów 1/10GBASE-T, 6 x 40G BASE-X QSFP+/2xQSFP28

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.

1. Typ i liczba portów:

- Minimum 48 porty 100/1000/10GBaseT,
- Minimum 6 porty 40GbE QSFP+/2 porty QSFP28.

2. Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management.

3. Port konsoli RS232 ze złączem DB9 lub RJ45.

4. Port USB 2.0.

5. Przepustowość minimum 1071 Mp/s dla pakietów 64 bajtowych, przy zachowaniu opóźnienia dla 10G nie mniejszego niż 2.5s.

6. Wydajność: minimum 1440 Gb/s (prędkość przełączania „wirespeed" dla każdego portu przełącznika),

7. Przełączanie w warstwie 2 i 3 modelu OSI.

8. Wielkość bufora pakietów (packet buffer): minimum 12MB.

9. Minimum 1G pamięci typu Flash.

10. Minimum 4GB pamięci operacyjnej.

11. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów).

12. Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza.

13. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.

14. Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie ze wspólnym zarządzaniem. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 320 portów 10GbE SFP+. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)).

15. Łączenie w stos z wykorzystaniem portów 10Gb, 40Gb i agregowanych portów 10Gb (w celu zwiększenia przepustowości w stosie).

16. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie

17. Tablica adresów MAC o wielkości minimum 208K pozycji.

18. Obsługa ramek Jumbo.

19. Obsługa Quality of Service.

20. Obsługa mechanizmów: strict priority (SP) queuing, weighted fair queuing (WFQ), weighted random early discard (WRED), SP+WFQ .

21. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol.

22. Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ.

23. Obsługa IGMP v1/v2/v3, IGMP Snooping v1/v2/v3, PIM DM, PIM SM, MLD snooping v1/v2 oraz IPv6 PIM Snooping.

24. Wsparcie dla FibreChannel over Ethernet (FCF/Transit/NPV).

25. Wsparcie dla Data Center Bridging (DCB):

• IEEE 802.1Qbb Priority Flow Control (PFC)

• Data Center Bridging Exchange (DCBX)

26. Routing IPv4 – statyczny i dynamiczny (min. RIP, IS-IS, OSPF, BGP).

27. Routing IPv6 – statyczny i dynamiczny (min. RIPng, IS-ISv6, OSPFv3).

28. Obsługa ECMP (Equal Cost Multi Path) .

29. Tablica routingu o pojemności co najmniej 16K wpisów.

30. Serwer DHCP, klient DHCP, obsługa opcji 82 (snooping i relay), DHCP Snooping.

31. Obsługa list ACL na bazie informacji z warstw 3/4 modelu OSI.

Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia

32. Obsługa standardu 802.1p.

33. Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p.

34. Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, remote mirroring

35. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x.

36. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS.

37. Zarządzanie poprzez port konsoli, SNMP v.1, 2c i 3, Telnet, SSH v.2.

38. Syslog.

39. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED.

40. Obsługa sFlow.

41. Obsługa NETCONF.

42. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3.

43. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter.

44. Obsługa Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) oraz kompatybilność z Precision Time Protocol (PTP) RFC 1855.

45. Obsługa OAM (IEEE 802.3ah).

46. Obsługa CFD (IEEE 802.1ag).

47. Modularny system operacyjny ze wsparciem dla In Services Software Upgrade (ISSU) i skryptów w języku Python.

48. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).

49. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).

50. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

51. Wysokość w szafie 19” – 1U.

52. Maksymalny pobór mocy nie większy niż 450W

53. Minimalny zakres temperatur pracy od 0°C do 40°C.

54. Minimum 5 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na wymianę na maksymalnie następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika (co najmniej 10 lat), również po wygaśnięciu kontraktu serwisowego.

55. Przełącznik powinien pochodzić z oficjalnego kanału dystrybucji producenta.

56. Przełącznik musi być fabrycznie nowy.

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 dostępu 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.

Pasma robocze

1. Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości:

a. 802.11ac/a/n (5 GHz),

b. 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. Musza 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.

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.

Uwaga:

Generalny Wykonawca na etapie realizacji wykona pomiary propagacji fal instalacji WiFi (uwzględniające aktualną architekturę i aranżację budynku) i w oparciu o te pomiary wykona aktualizację rozmieszczenia Access Point-ów (AP). Zestawienie materiałów uwzględnia 5% zapas Access Point-ów, który Wykonawca może wykorzystać w ceku uzupełnienia sieci AP. Niewykorzystane urządzenia Wykonawca zobowiązany jest przekazać Zamawiającemu.

Urządzenie w celu zapewnienia funkcjonalności NGFW w ramach sieci wewnętrznej, jak i do podłączenia do sieci Internet czy sieci zewnętrznych

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:

   a. routera (tzn. w warstwie 3 modelu OSI),

   b. przełącznika (tzn. w warstwie 2 modelu OSI),

   c. 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)

   d. 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:

   a. tablic routingu przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.

   b. Polityk bezpieczeństwa obejmujących:

      i. System IPS,

      ii. System ochrony antymalware/antyspyware,

      iii. System ochrony antywirus.

   c. Koncentratorów VPN dla zdalnego dostępu.

Wymagania dot. platformy, wymagania wydajnościowe

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

   a. 8 portów Gigabit Ethernet 1000BASE-T,

   b. 8 portów Gigabit Ethernet SFP.

   c. 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

6. 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).

7. Polityka zabezpieczeń firewall musi uwzględniać:

   a. strefy bezpieczeństwa,

   b. adresy IP klientów i serwerów,

   c. protokoły i usługi sieciowe,

   d. aplikacje,

   e. kategorie URL,

   f. użytkowników aplikacji,

   g. reakcje zabezpieczeń,

   h. rejestrowanie zdarzeń i alarmowanie,

   i. zarządzanie pasmem w sieci w oparciu o:

   a. priorytet,

   b. pasmo gwarantowane,

   c. pasmo maksymalne,

   d. oznaczenia DiffServ.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

Wymaganie dotyczące identyfikacji użytkowników

1. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci

2. System zabezpieczeń firewall musi zapewniać integrację z:

   a. Active Directory,

   a. Ms Exchange,

   b. Citrix,

   c. LDAP,

   d. 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 dot. 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.

a. Polityki definiujące powinny umożliwiać wykorzystanie

i. adresów źródłowych,

ii. adresów docelowych,

iii. użytkowników,

iv. numerów portów usług

v. kategorie URL.

b. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia

i. RADIUS,

ii. TACACS+,

iii. LDAP,

iv. Kerberos,

v. 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 zmian w pojedynczym systemie/kontekście wpływało 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:

a. ruchu sieciowym,

b. aplikacjach,

c. zagrożeniach

d. 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.

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.

5.7 System Kontroli Dostępu

Przedmiotem niniejszego opracowania jest projekt wykonawczy systemu kontroli dostępu (SKD), dla drugiego etapu budowy centrum kliniczno-dydaktycznego uniwersytetu medycznego w Łodzi wraz z akademickim ośrodkiem onkologicznym.

Zakres instalacji

W ramach projektowanych obiektów, założono stworzenie spójnego systemu kontroli dostępu zabezpieczającego dostęp do poszczególnych stref i pomieszczeń, stanowiącego integralną część systemu stosowanego przez Uniwersytet Medyczny w Łodzi.

Instalacja korzystać będzie ze wspólnej bazy danych oraz kart studentów i pracowników naukowych Uniwersytetu Medycznego w Łodzi i musi być kompatybilna z istniejąca instalacją.

Wszystkie elementy systemu zaprojektowano w oparciu o rozwiązanie firmy SALTO System jako kompatybilne z istniejącym systemem.

Ogólna charakterystyka systemu

Projektowany system kontroli dostępu umożliwi swobodne poruszanie się pracowników, wyłącznie po strefach dla nich przeznaczonych. Ogranicza to dostęp osób nieupoważnionych do poszczególnych stref i pomieszczeń..

Proponowany system bazuje na przewodowych i bezprzewodowych czytnikach zbliżeniowych oraz na bezprzewodowej technologii okuć on-line, w standardzie Mifare/Desfire, wykorzystujących Sieć Wirtualną Salto.

Poszczególne części obszaru kontrolowanego podzielone są na strefy oddzielone od siebie nadzorowanymi przejściami, zlokalizowanymi przy wejściach do poszczególnych stref. Strefy wyposażono w przejścia kontrolowane jednostronnie, które dają możliwość określenia rejestracji zdarzeń posiadacza określonej karty (system rejestruje gdzie dana osoba wchodzi). W pamięci kontroli dostępu przechowywane są informacje o uprawnieniach użytkownika systemu oraz o wszystkich zdarzeniach w systemie.

W ramach części hotelowej, możliwe będzie również stosowanie kluczy mobilnych działających w oparciu o dowolny smartphone z systemem operacyjnym Android lub OS, które działają równolegle ze standardowymi kartami oraz tagami Mifare.

Struktura i elementy składowe systemu

Czytniki ścienne

Czytniki zapewniają odczyt informacji z kart elektronicznych i komunikację poprzez kontroler z systemem. Wykorzystanie protokołów szyfrujących gwarantuje bezpieczną komunikację pomiędzy czytnikiem, kluczem i kontrolerem.

Parametry techniczne:

- Kompaktowa, wąska obudowa,
- Sygnalizacja optyczna I akustyczna,
- Maksymalny dystans pomiędzy kontrolerem a czytnikiem - 400m,
- Współpracuje z kontrolerami z serii XS4,
- Wymiary: 100x34,5x15mm

Czytniki należy montować na ścianie obok chronionych drzwi na wysokości około 1,4m od podłogi. Podczas montażu czytnika należy pamiętać o tym aby nie montować ich bezpośredniego na elementach metalowych co może radykalnie wpłynąć na zasięg odczytu kart zbliżeniowych tagów.

Uwaga: Ostateczną wysokość montażu czytników należy uzgodnić z Użytkownikiem, biorąc pod uwagę obsługę systemu przez osoby niepełnosprawne.

Okucia hotelowe

W części przeznaczonej na hostel, przewidziano zastosowanie okuć serii XS4, w wersji z mechaniczną funkcją prywatności i z możliwością zastosowania kluczy mobilnych JustIN.

Funkcja prywatności pozwala na ograniczenie dostępu osób niepowołanych, gdy gość sobie tego nie życzy, jednocześnie pozwalają na otwarcie drzwi przez uprawniony personel, pomimo aktywowania funkcji prywatności.

Zasilanie okuć będzie zagwarantowane dzięki zestawowi baterii 3x AAA. Producent przewiduje do 40 000 otwarć na jednym zestawie baterii.

Parametry techniczne okuć:

- Technologia odczytu – 13,56 MHz RFID, ISO14.443A, ISO 14.443B oraz ISO 15.693 Mifare, Mifare plus, DESFire, DESFireEV1;
- Zgodne z Bluetooth Low Energy (BLE), oraz Near Field Comunication (NFC);
- Kontaktronu do monitorowania stanu drzwi (w wersji Wireless on-line);
- Zasilanie: standardowe baterijne alkaliczne LR03 AAA (3 szt.) – 50.000 (3- 5 lat pracy);
- Temperatura pracy -20 – 60 ^{o}C;
- Odporność ogniowa wg. EN1634 EI 120;

Elementem pośredniczącym w komunikacji pomiędzy okuciami a serwerem systemowym będą Gatewaye oraz Nody komunikacyjne w technologii BlueNet (opartej o komunikacje Bluetooth Low Energy).

Kontrolery sterujące

Do podłączenia czytników, wykorzystane zostaną dedykowane przewodowe kontrolery sterujące. Serwer będzie łączył się z kontrolerami sterującymi CU42E0 poprzez sieć Ethernet, następnie do każdego zestawu 4 kontrolerów CU4200 poprowadzona zostanie magistrala RS485.

Zasilanie kontrolerów sterujących odbywa się za pośrednictwem zasilaczy sieciowych dostarczanych w komplecie z kontrolerem i szczelną obudową montażową.

Montaż kontrolerów sterujących wraz z zasilaczami przewidziano w pomieszczeniach technicznych.

Okablowanie

Dobór okablowania

Instalacja kablowa SKD, będzie opierała się na przewodach sterujących/sygnałowych, których typy i ilości (w zależności od rodzaju przejścia kontrolowanego wskazano na schematach blokowych.

Elementy sieciowe systemu będą podłączone od obiektowej instalacji okablowania strukturalnego, którą opisano w osobnym rozdziale.

Prowadzenie okablowania

Okablowanie należy prowadzić podtynkowo w ścianach i podłogach, w rurach PCV sztywnych lub peszlach, a w przestrzeniach międzysufitowych na korytach kablowych lub w rurach PCV. W przestrzeniach technicznych dopuszcza się prowadzenie okablowania natynkowo.

Odejścia do urządzeń prowadzić podtynkowo, wypusty muszą uwzględniać stosowną rezerwę w miejscach montażu urządzeń. Ostateczne prowadzenie tras kablowych należy ustalić podczas wykonania instalacji.

Trasowanie tras kablowych na potrzeby systemu kontroli dostępu (SKD), należy wykonać z uwzględnieniem innych branż i tam gdzie to możliwe korzystać z tych samych tras kablowych, zachowując stosowne odległości między przewodami sygnałowymi a zasilającymi. W przypadku gdy wypełnienie rury PCV/peszla, w której prowadzone jest okablowanie nie zapewni swobodnej możliwości dołożenia w przyszłości dodatkowego kabla tego samego rodzaju, który został ułożony należy położyć dodatkową rurę PCV/peszel na identycznej trasie. Wszystkie przewody należy wyprowadzić z rezerwą zapewniającą prawidłowy montaż i podłączenie urządzeń.

Oprogramowanie

Projektowany System Kontroli Dostępu, będzie stanowił rozbudowę istniejącej instalacji SKD i będzie funkcjonował jako integralna część systemu stosowanego przez Uniwersytet Medyczny w Łodzi.

Instalacja korzystać będzie ze wspólnej bazy danych oraz kart studentów i pracowników naukowych Uniwersytetu Medycznego w Łodzi.

Dla projektowanej części systemu, przewidziano odpowiednią ilość nowych licencji, które umożliwią rozbudowę istniejącego stanowiska zarządzania SKD.

Integracja z istniejącym systemem kontroli dostępu

W istniejących budynkach funkcjonuje już system kontroli dostępu SALTO. Projektowane urządzenia uwzględniają wymaganą integrację z obecnym systemem.

Możliwość rozbudowy systemu

Dobór oraz ilość elementów centralnych projektowanego Systemu Kontroli Dostępu, uwzględnia możliwość rozbudowy instalacji o kolejne czytniki i kontrolery co znacznie ułatwia możliwość wprowadzania zmian w konfiguracji systemu na wypadek przebudowy aranżacji obiektu lub przeznaczenia poszczególnych pomieszczeń.

Projektowana konfiguracja systemu pozwala na etapowe wykonywanie instalacji SKD.

Integracja z innymi instalacjami

W projektowanym obiekcie będzie możliwa pełne zintegrowanie elementów systemu kontroli dostępu zarówno z systemami zarządzania budynkiem (BMS), jak i pozostałymi systemami bezpieczeństwa funkcjonującymi w obiekcie, jak np. monitoring wizyjny CCTV IP, czy system alarmowy SSWiN.

Wytyczne i uwagi

- Wszystkie drzwi objęte Systemem Kontroli Dostępu należy wyposażyć w elektromagnetyczne zaczepy rewersyjne.

- Należy doprowadzić zasilanie 230V do wszystkich zasilaczy sieciowych wchodzących w skład zestawu kontrolerów sterujących. System będzie zasilany z rozdzielnic zasilania gwarantowanego.
- Zwalnianie kontroli dostępu w przypadku pożaru, będzie realizowana poprzez System Sygnalizacji Pożarowej (SSP). Sygnały zwalniające z modułów SSP będę przekazywane bezpośrednio na zaczepy ektromagnetyczne.

Zestawienie materiałów podstawowych SKD

Lp.	Model	Opis	Ilość	Jednostka
1	DOORLICENSE01	Oprogramowanie i licencja	210	szt.
Lp.	**Model**	**Opis**	**Ilość**	**Jednostka**
1	CU42E0T	Kontroler sterujący z zasilaczem sieciowym	36	szt.
2	CU4200T	Kontroler sterujący z zasilaczem sieciowym	96	szt.
3	WRDB0M4B	Czytnik ścienny	232	szt.
4	D-110	Przycisk ewakuacyjny	44	szt.

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.

5.8 System CCTV

Zakres instalacji

Projektowana instalacja telewizji dozorowej, będzie monitorowała wyznaczone przestrzenie wewnątrz obiektów oraz otaczający je teren zewnętrzny.

Ogólna charakterystyka systemu

Projektuje się zastosowanie systemu wykorzystującego do komunikacji sieć Ethernet. Technologia ta zapewni możliwość łatwej rozbudowy systemu oraz możliwość udostępnienia danych dowolnej ilości użytkowników w zależności od przyszłych potrzeb użytkownika.

W warstwie urządzeń przechwytujących obraz, zastosowane będą kamery odpowiednie do warunków pracy i indywidualnie dobrane do pełnionych funkcji i obszarów obserwacji. Kamery instalowane będą na, ścianach i sufitach. Sygnał z kamer agregowany będzie w pośrednich punktach dystrybucyjnych i doprowadzono do głównego punktu dystrybucyjnego.

Kamery chroniące otoczenie budynku zlokalizowane będą na elewacjach budynków i słupach oświetleniowych.

Struktura i elementy składowe systemu

W skład instalacji telewizji dozorowej, wchodzą urządzenia takie jak kamery, rejestratory oraz stacja robocza z monitorami do podglądu.

Kamery instalowane będą wewnątrz budynku w korytarzach, poczekalniach, na klatkach schodowych, na wybranych oddziałach oraz tam gdzie może wystąpić potrzeba monitorowania danego obszaru a także otoczenia budynku.

Projektuje się zastosowanie kamer CCTV zapewniając wysoką jakość obrazu oraz wiele dodatkowych funkcji wspomagających w trudnych warunkach pracy.

Kamery

Do monitorowania przestrzeni wewnątrz budynku, projektuje się kamery kopułkowe o poniższych parametrach technicznych:

- Rozdzielczość 4MP (max. 2688x1520@25kl/s)
- przetwornik: 1/2.5” Progressive Scan CMOS
- czułość: 0.008Lux@ F1.2 (wł. AGC), 0.011Lux@ F1.4 (wł. AGC), 0 Lux z IR
- zasięg IR EXIR do 40m, dzień/noc ICR
- obiektyw: 2.7 to 13.5 mm/F1.4, kąt poziomy: od 116 do 30°
- Kompresja: H.265+/H.265/H.264+/H.264/MJPEG
- Funkcje: trzy strumienie, WDR: 120dB, 3D DNR, HLC, BLC, ROI: 1 obszar, detekcja przekroczenia linii, detekcja naruszenia strefy, nagła zmiana sceny, wykrycie twarzy
- Klasa szczelności: IP66
- Klasa odporności mechanicznej: IK10
- 3-osiowa regulacja położenia
- Wbudowany slot na kartę microSD do 128GB
- wejście/ wyjście alarmowe 1/1
- Temperatura pracy: -30 °C to +60 °C
- Wymiary: Φ 153.4 x133,1 mm
- Waga 1287g
- Zasilanie 12VDC/PoE

Do monitorowania przestrzeni wymagających bardziej precyzyjnych funkcji nadzoru i identyfikacji przewidziano kamery wykorzystujące algorytmy detekcji zdarzeń i wykrywania twarzy o poniższych parametrach technicznych:

- Rozdzielczość: 4MP (max. 2560 × 1440 @ 25kl/s),
- Przetwornik: 1/1.8” Progressive Scan CMOS,
- Czułość: 0.002Lux@ F1.2 (wł. AGC),
- Migawka: 1-1/100000s,
- Obiektyw: motozoom 2.8-12mm, Poziomy kąt widzenia: 109.2° ~ 38.9°,
- Zasięg oświetlacza IR: do 30 metrów,
- Pięć zdefiniowanych strumieni i do pięciu strumieni spersonalizowanych,
- Kompresja obrazu: H.265+/H.265/H.264+/H.264,MJPEG,
- Funkcje: WDR 140dB, 3D DNR, BLC, HLC, Defog, EIS, ROI,
- Funkcje SMART: Ochrona perymetryczna, detekcja zdarzeń, wykrywanie twarzy,

- Wbudowany slot na kartę microSD/SDHC/SDXC do 256 GB,
- Wejście/wyjście audio: 1/1,
- Wejście/wyjście alarmowe: 1/1,
- Przycisk Reset,
- Temperatura pracy: -30 °C - 60 °C,
- Zasilanie: 12V DC; PoE (802.3af, class 3),
- Klasa odporności mechanicznej: IK10,
- Wymiary: Φ140.5 × 122.6 mm,
- Waga: 950 g.

Rejestratory

W obiekcie zainstalowany zostanie system rejestracji wraz z urządzeniami sieciowymi, oparty o cyfrowe rejestratory, przeznaczone do rozbudowanych systemów monitoringu wizyjnego. Rejestrator umożliwia zapis, podgląd oraz odtwarzanie obrazu z maksymalnie 64 kamer IP o rozdzielczości sięgającej 12 Mpx. Parametry techniczne:

- wejścia wideo: 64x kanały IP,
- wyjścia wideo: 2x VGA, 2x HDMI (4K UHD),
- maks. rozdzielczość nagrywania: 4000x3000 (12Mpx),
- maks. bitrate: 320Mbit (wej.), 256Mbit (wyj.),
- format kompresji: H.265+/H.265/H.264/H.264+/MPEG4,
- interfejs: 1x RS485, 1x RS232, 1x eSata,
- wejście/wyjście audio: 1/2 (RCA),
- wejścia/wyjścia alarmowe: 16/4,
- interfejs sieciowy: 2x Ethernet 10/100/1000Mbps,
- obsługa dysków: 8x HDD Sata III (max. 80TB),
- wsparcie dla kamer z wbudowaną analityką obrazu,
- zgodność ze standardem: ONVIF, RSTP,
- obsługa połączeń P2P,
- obsługa RAID 0, 1, 5, 10,
- inteligentne funkcje analizy wideo (VCA),
- synchroniczne odtwarzanie do 16 kanałów wideo,
- niezależna praca wyjść HDMI/VGA,
- jeden dwukierunkowy tor audio – interkom,
- rejestracja dźwięku z 64 kamer IP.

Dyski

Dobór i ilość dysków do projektowanego systemu określono po wykonaniu obliczeń z uwzględnieniem założonej rozdzielczości, poklatkowości, kompresji i wymganaego czasu przechowywania zapisu z kamer.
W projektowanym systemie przewidziano zastosowanie dysków ST8000VX0002, przeznaczony do pracy ciągłej. Parametry techniczne:

- Rodzaj Dysku: wewnętrzny,
- Typ dysku: HDD
- Interfejs: SATA 3
- Max przepustowość: 6 Gbps
- Prędkość obrotowa: 7200RPM
- Format fizyczny: 3.5"

- Pojemność: 8 TB
- Zasilanie: pobór mocy: 5.2 W
- Pamięć podręczna: 64 MB
- Waga: 610 g

Stacja operatorska

Na potrzeby obsługi i podglądu systemu monitoringu, przewidziano stację operatorską o poniższych parametrach. Parametry techniczne:

- Typ obudowy komputera: mid tower
- Nazwa rodziny produktów: Dell Alienware Aurora R7
- Procesor: Intel Core i7-8700 sześciordzeniowy
- Pojemnośc pamięci RAM: 16GB DDR4 2666 mhz
- Wyjścia: 4x Displayport
- Dyski: 1TB SATA 7200 rpm + 16gb Intel optane
- Łączność LAN 10/100/1000, WiFi Killer 1535 + Bluetooth 4.1
- Zewnętrzna karta graficzna: Nvidia GeForce GTX 1070, 8GB GDDR5
- System operacyjny Windows 10 Proffesional PL 64 bit
- Moc zasilacza 460W

Okablowanie

System będzie wykorzystywał projektowane okablowanie strukturalne. Zasilanie kamer zostanie zrealizowane z wykorzystaniem technologii PoE.

Prowadzenie okablowania

Okablowanie należy prowadzić podtynkowo w ścianach, w rurach PCV sztywnych lub peszlach, a w przestrzeniach międzysufitowych na korytach kablowych lub w rurach PCV. W przestrzeniach technicznych dopuszcza się prowadzenie okablowania natynkowo.

Odejścia do urządzeń prowadzić podtynkowo, wypusty muszą uwzględniać stosowną rezerwę w miejscach montażu urządzeń. Ostateczne prowadzenie tras kablowych należy ustalić podczas wykonania instalacji.

Trasowanie tras kablowych na potrzeby systemu telewizji dozorowej (CCTV), należy wykonać z uwzględnieniem innych branż i tam gdzie to możliwe korzystać z tych samych ciągów kablowych, zachowując stosowne odległości między przewodami sygnałowymi a zasilającymi. W przypadku gdy wypełnienie rury PCV/peszla, w której prowadzone jest okablowanie nie zapewni swobodnej możliwości dołożenia w przyszłości dodatkowego kabla tego samego rodzaju, który został ułożony należy położyć dodatkową rurę PCV/peszel na identycznej trasie. Wszystkie przewody należy wyprowadzić z rezerwą zapewniającą prawidłowy montaż i podłączenie urządzeń.

Oprogramowanie

Do projektowanego systemu CCTV dobrano oprogramowanie zarządzające, które pozwoli na zarządzanie monitoringiem wideo (VSM) oraz wizualizację rejestratorów w sieciach IP, z możliwością podłączenia do 300 kamer.

Zestawienie elementów

Elementy centralne:

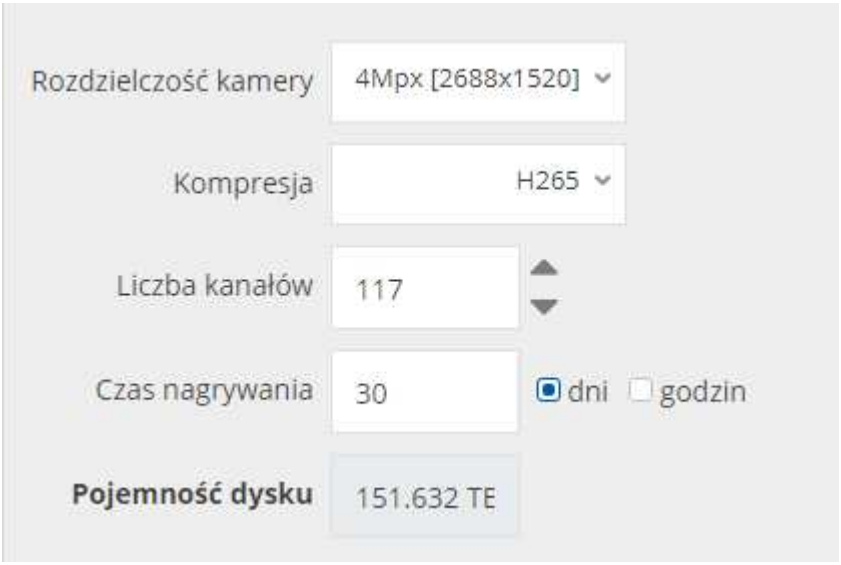
Lp.	Model	Opis	Ilość	Jednostka
1	DS-9664NI-I8/R	Rejestrator NVR 64 kanałowy	2	szt.
2	iDS-9616NXI-I8/8F(B)	Rejestrator NVR 8 kanałowy z funkcjami analizy obrazu	1	szt.
3	ST8000VX0002	Dysk 3,5” 8TB do pracy ciągłej	19	szt.
4	SERWER KLIENT	Stacja robocza	1	szt.
5	DS-D5032FC-A	Monitor LED 23,6”	4	szt.

Kamery:

Lp.	Model	Opis	Ilość	Jednostka
1	DS-2CD3745G0-IZS(2.7-13.5mm)	Kamera w obudowie kopułkowej	109	szt.
2	DS-2CD7146G0-IZS(2.8-12mm)	Kamera w obudowie kopułkowej	8	szt.

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.

Poniżej przedstawiono przykładową kalkulację przestrzeni dyskowej, jaka niezbędna będzie do prawidłowej obsługi i archiwizacji nagrań z kamer do monitoringu:



Stanowisko monitoringu

Przewiduje się stanowiska monitoringu w pomieszczeniach ochrony:

- A1 – pom. P01.PT.42
- A2 – pom. P00.PP.72

5.9 System Sygnalizacji Włamania i Napadu

Ogólne założenia

Projektuje się instalację sygnalizacji włamania obejmującą pomieszczenia wskazane w części rysynkowej opracowania oraz w poniższym zestawieniu. 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

Odpowiednie rozmieszczenie czujek zapewni wytworzenie stref ochronnych, które obejmują pomieszczenia określone przez Inwestora. Rozmieszczenie elementów sytemu pokazano na podkładach budowlanych.

	L.p	Nr. Pom	Nazwa pom.	Kontaktrony	Czujki	Klawiatura	Ekspander	Moduł IO
A1	1	P7.UR.44	Mag. leków	1	1	1	1	0
	2	P10.CO.48	Mag. leków	1	1	1	1	0
	3	P10.CO.43	Mag. leków	1	1	1	1	0
	4	P10.CO.61	Mag. leków	1	1	1	1	0
	5	P3.RAD.19	Mag. leków	1	1	1	1	0
	6	P6.GO.35	Mag. leków	1	1	1	1	0
	7	P01.SW.77	Mag. depozytów	1	1	1	1	0
	8	P01.SW.42	Pom. monitoringu	2	1	1	0	0
	9	P0.CJD.32	Pom. przyg. leków	1	1	1	1	0
	10	P01.AK.1	Mag. apteki	1	1	1	1	0
	L.p	Nr. Pom	Nazwa pom.	Kontaktrony	Czujki	Klawiatura	Ekspander	Moduł IO
A2	1	P00.CBK.1c	Archiwum podręczne	1	1	1	1	0
	2	P00.CBK.11	Mag. leków	1	1	1	1	0
	3	P00.CBK.19	Archiwum	1	1	1	1	0
	4	P00.IP.60	Mag. leków	2	1	1	1	0
	5	P00.IP.72-2	Pom. ochrony-2	2	1	1	0	0
	6	P00.IP.81	Mag. depozyty	1	1	1	1	0
	7	P00.PL.7	Archiwum	1	1	1	1	0
	8	P00.POR.6	Archiwum podręczne	1	1	1	1	0
	9	P00.TK.14	Gab. komora hiperbaryczna	3	1	1	1	0
	10	P1.ADM.18	Kasa	1	1	1	0	0
	11	P1.ADM.68	Archiwum B	1	1	1	1	0
	12	P1.ADM.92	Sekcja ds. obronnych / oc	1	1	1	1	0
	13	P1.ADM.95	Archiwum	1	1	1	1	0
	14	P1.AP.1	Komora wydaw.	1	1	1	1	1
	15	P1.AP.2	Ekspedycja	1	1	1	1	0
	16	P1.AP.4	Pom. administracyjne	1	1	1	1	0
	17	P1.AP.5	Pom. szkoleniowe	1	1	1	0	0
	18	P1.AP.10	Mag. cytostatyków	1	2	1	1	1
	19	P1.AP.11	Izba recepturowa	1	1	1	1	1
	20	P1.AP.16	Mag. lekow do badan klinicznych	1	1	1	0	0
	21	P1.AP.17	Prac. Leków cytostatycznych	2	1	1	1	1
	22	P1.AP.22	Mag. leków	2	2	1	1	2
	23	P1.AP.25	Gab. kierownika	1	1	1	0	0
	24	P1.AP.27	Laboratorium z. pozajelitowego	2	2	1	0	0
	25	P1.AP.35	Receptura jał.	2	2	1	0	0
	26	P1.AP.44	Ekspedycja unit dose	5	2	1	1	1
	27	P1.AP.47	Mag. Chłodnia	2	1	1	0	0
	28	P1.AP.52	Prac. Leków cytostatycznych	2	1	1	0	0
	29	P1.AP.59	Komunikacja	5	3	1	0	0
	30	P1.AP.60	Komunikacja	7	4	1	1	0
	31	P1.AP.63	Kierownik pracowni cyt.	1	1	1	0	0
	32	P01.BO.17	Mag. leków	1	1	1	1	0
	33	P02.AP.1	Mag. Sprzętu jednorazowego użytku	3	1	1	0	0
	34	P02.AP.2	Mag. Opatrunkow i pieluch	3	2	1	1	2
	35	P02.AP.3	Mag. Płynów	3	1	1	0	0
	36	P02.AP.4	Mag. implantów ortopedycznych	3	1	1	0	0
	37	P02.AP.5	Mag. implantów kardiologicznych	3	2	1	0	0
	38	P02.AP.6	Mag. Środków dezynfekujących	1	1	1	1	2
	39	P02.AP.7	Komora przyjęć	4	1	1	0	0
	40	P02.AP.8	Komunikacja	2	2	1	0	0
	41	P02.AP.10	Archiwum	1	1	1	0	0
	42	P02.AP.11	Mag. Mat. Łatwopal.	1	1	1	0	0
	43	P02.AP.12	Dystrybucja komercyjna	3	2	1	1	1
	44	P02.AP.20	Mag. implantów ortopedycznych	2	1	1	0	0
	45	P02.AP.21	Mag. Płynów	3	2	1	0	0
	46	P02.AP.22	Mag. Opatrunkow i pieluch	5	2	1	1	1
	47	P02.AP.23	Mag. Sprzętu jednorazowego użytku	3	2	1	0	0
	48	P02.AP.24	Komunikacja	4	3	1	1	0
	49	P02.BK.3-2	Bank krwi-2	2	1	1	1	0
	50	P02.MB.12	Archiwum podręczne	1	1	1	1	0
	51	P02.MC.3-2	Strefa skład. tow. wielkogabarytowych-2	2	2	1	1	0
	52	P02.PT.15-1	Mag. depozyty-1	1	1	1	1	0

Na szaro zaznaczono obszary wyłączone z zakresu niniejszego opracowania.

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 centrale alarmowe. 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.

Okablowanie

Centrala SSWiN zostanie podłączona do przełącznika sieci systemów bezpieczeństwa poprzez okablowanie LAN systemu bezpieczeństwa – kabel F/FTP 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.

Projektuje się sygnalizatory optyczno-akustyczne, które będą sygnalizowały wystąpienie alarmu zarówno wewnątrz jak i na zewnątrz chronionego obiektuProjekt przewiduje zainstalowanie 10 przycisków napadowych, których szczegółową lokalizację należy ustalić na etapie realizacji inwestycji zgodnie z ostateczną aranżacją wnętrz i układem funkcjonalnym zaakceptowanymi przez Inwestora. Na potrzeby podłączenia przycisków napadowych przewidziana jest rezerwa wejść w poszczególnych ekspanderach wejść.

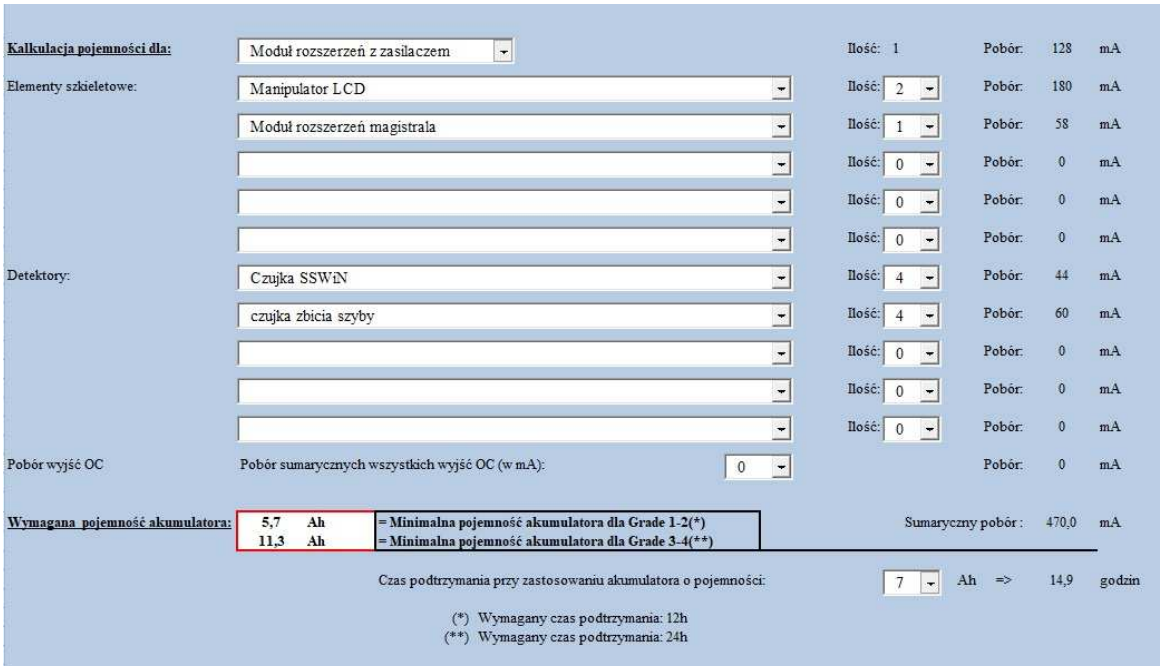
Sygnalizację alarmu napadowego przewiduje się w pomieszczeniu ochronny za pomocą dodatkowego sygnalizatora optycznego.

Centrala zostanie doposażona w akumulator pozwalający na podtrzymanie zasilania systemu przez czas niezbędny do uruchomienia zasilania rezerwowego. 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 pozwalające na podtrzymanie zasilania systemu przez czas niezbędny do uruchomienia zasilania rezerwowego. Poniżej przykładowe wyliczenie:



Powyższe wyliczenia należy traktować jako przykładowe, a dobory takich elementów jak pojemności akumulatorów każdego z zasilaczy indywidualnie Generalny Wykonawca zobowiązany jest wykonać na etapie realizacji w oparciu o dane Producenta systemu zaakceptowanego przez Inwestora i Nadzór Autorski.

5.10 System telewizji użytkowej RTV

W obiekcie projektuje się jedynie przygotowanie pod instalację IPTV. W tym celu przewidziano dedykowane linki, osobne patchpanele oraz rezerwę miejsca w szafach RACK. Zgodnie z wymogiem Inwestora obsługa systemu telewizji w Szpitalu zostanie zlecona zewnętrznej firmie. Okablowanie oraz gniazda ujęto w systemie okablowania strukturalnego.

5.11 System Wykrywania Gazów

Detekcja wodoru

W pomieszczeniach UPS oraz baterii centralnej projektuje się system wykrywania i pomiaru wodoru oparty na czujnikach H2. System powinien 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. System powinien być wyposażony 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. Detektory powinny 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 oraz w BMS, 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.

Detekcja dwutlenku węgla

W pomieszczeniu rozprężalni CO2 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. Detektor należy wyposażyć w wymienny elektrochemiczny sensor dwutlenku węgla. Czujnik zasilany będzie z rozdzielnicy wg projektu elektrycznego należy go 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.

Detekcja metanu

W przypadku konieczności wykonania detekcji metanu należy wykonać Aktywny System Bezpieczeństwa Instalacji Gazowej w miejscu umożliwiającym łatwy dostęp przez osoby obsługujące System. należy zainstalować obok istniejącego MD-4.Z

Czujniki Gazu:

Projekt przewiduje zainstalowanie detektorów metanu, których szczegółową lokalizację należy ustalić wg projektu branży sanitarnej.

Gazowy zawór odcinający:

Gazowy zawór odcinający MAG zainstalowany zgodnie z projektem instalacji gazowej, należy podłączyć z centralą systemu zabezpieczenia gazowego za pomocą przewodu zainstalowanego w korytach lub rurkach elektroinstalacyjnych.

Uwagi:

Wszystkie instalacje wykonać zgodnie z obowiązującymi przepisami dotyczącymi wykonywania instalacji elektrycznych. Poprawność wykonania instalacji potwierdzić protokółami z badania stanu izolacji i ochrony przeciwporażeniowej. Przy wykonywaniu instalacji należy przestrzegać zasad BHP. Przed przystąpieniem do wykonywania robót kierownik robót zobowiązany jest do sporządzenia planu BIOZ, oraz szczegółowego harmonogramu robót uzgodnionego z Użytkownikiem obiektu. Szczegółowych podłączeń należy dokonać zgodnie z dokumentacją producenta urządzeń.

Ze względu na zapewnienie maksymalnego bezpieczeństwa zaleca się powiązanie SSP i systemu detekcji metanu komunikacją dwustronną.

5.12 System Przyzywowy

Założenia projektowe

Projekt przewiduje instalację systemu przyzywowego i komunikacji szpitalnej w całym obiekcie szpitalnym.

System przyzywowy musi zostać cyfrowo połączony z nowym i istniejącym w szpitalu systemem sygnalizacji pożarowej w celu przekazywania szczegółowych informacji o zagrożeniu pożarowym a także w celu powiadomienia personelu przemieszczającego się po obiekcie do przygotowania ewakuacji pacjentów podczas pożaru. Ze względu na brak w salach chorych dźwiękowego systemu ostrzegawczego (DSO) umożliwi grupowe ogłaszanie komunikatów bezpośrednio przy łóżkach pacjentów a także na terminalach zainstalowanych przy drzwiach wejściowych do sal i pomieszczeń personelu.

System przyzywowy zostanie integrowany z istniejącą na obiekcie centralą telefoniczną w standardzie SIP w celu odbierania informacji o przywołaniach, prowadzenia rozmowy a także akceptacji lub kasowania połączeń np. na telefonach mobilnych typu DECT lub VoIP.

W projekcie przewidziano urządzenia systemu przyzywowego i systemowe przełączniki sieciowe (switch) posiadające certyfikaty dla szpitalnych systemów przywoławczych i komunikacji zgodnie z normą DIN VDE 0834 część 1 i 2.

System zapewnia cyfrową, obustronną komunikację głosową jednocześnie z każdą osobą w pokoju wyposażoną w terminal pacjenta, funkcje nadawania komunikatów np. poinformowanie pacjentów o czynnościach ewakuacyjnych podczas pożaru, poinformowanie o obchodzie lekarskim, wyświetlanie informacji tekstowych zgodnych z wymaganiami

użytkownika i przekierowywania przywołań / eskalowanie przywołań na inne wskazane oddziały lub urządzenia np. telefony przenośne.

Projektowany system zapewnia rozwój funkcjonalności wraz z rozwojem produktu poprzez automatyczną aktualizację firmware przy zmianach oprogramowania.

System jest skalowalny a producent systemu gwarantuje, że urządzenia są kompatybilne z poprzednimi generacjami urządzeń (minimum jedną generacją urządzeń). Kompatybilność jest potwierdzona dotychczasową minimum 20 letnią polityką firmy, co gwarantuje inwestorowi obniżenie kosztów eksploatacji i rozbudowy systemu w przyszłości.

Minimalne parametry techniczne i funkcjonalne systemu

- system cyfrowy bazujący na urządzeniach IP (Internet Protocol) zapewniający łatwość rozbudowy, skalowalność zgodnie z wymaganiami użytkownika,
- system przyzywowy ma zachować funkcjonalność przy uszkodzeniu serwera tzn. że urządzenia systemu przyzywywowego pracują bez zmian i przekazują informacje cyfrowe w ramach zaprogramowanych oddziałów
- cyfrowy standard dźwięku i komunikacji głosowej – system ma zapewniać funkcję prowadzenia rozmowy z każdą osobą w pokoju/ sali w tym samym czasie tzn. słuchawkami pacjenta (terminalami pacjentów) przy łóżkach lub terminalem komunikacyjnym przy drzwiach wejściowych w pokoju,
- prowadzenie rozmów pomiędzy pacjentem a personelem w sposób dyskretny przez słuchawkę i/lub w sposób głośnomówiący bez podnoszenia słuchawki z uchwytu za pomocą terminali komunikacyjnych,
- prowadzenie rozmów pomiędzy personelem w punkcie pielęgniarskim a pacjentem w sposób dyskretny przez słuchawkę terminala oddziałowego jak również w sposób głośnomówiący bez podnoszenia słuchawki (o sposobie rozmawiania decydują pielęgniarka w punkcie pielęgniarskim),
- słuchawki przy łóżkach muszą umożliwiać definiowanie dowolnych dodatkowych min. 5 przywołań z różnymi priorytetami np.
  - przywołanie salowej (przywołanie standardowe),
  - przywołanie pielęgniarki (przywołanie standardowe),
  - przywołanie dodatkowej pielęgniarki (przywołanie standardowe),
  - przywołanie lekarza (przywołanie standardowe),
  - alarm krytyczny (przywołanie standardowe) – widziane przez zespół pielęgniarek i lekarzy
  - pielęgniarka noworodkowa (przywołanie dodatkowe),
  - chirurg -można zdefiniować specjalizację lekarza leżeli będzie potrzeba rozróżniania lekarzy (przywołanie dodatkowe),
  - anestezjolog -można zdefiniować specjalizację lekarza leżeli będzie potrzeba rozróżniania lekarzy (przywołanie dodatkowe),
  - resuscytacja (jeżeli zespół ma zabrać jakieś urządzenia, przywołanie wówczas może trafić personelu pielęgniarskiego i lekarskiego),
  - krwotok (jeżeli zespół ma zabrać jakieś urządzenia, przywołanie wówczas może trafić personelu pielęgniarskiego i lekarskiego),
  - itp.
- cyfrowy standard ogłaszania komunikatów (zapowiedzi) do wszystkich urządzeń systemu przyzywowego z funkcją komunikacji głosowej (do wszystkich na oddziale), tylko do pielęgniarek, tylko do lekarzy, do całego personelu – funkcja istotna w przypadku poinformowania pacjentów nie mogących się samodzielnie przemieszczać

o czynnościach które wykona personel; podczas normalnej pracy funkcja umożliwia poinformowanie pacjentów o zbliżającym się obchodzie, o wydawaniu posiłków; zapowiedzi po grup personelu umożliwiają sprawniejsze przywoływanie konkretnych osób nie wyposażonych w telefony, w przypadku zagrożenia np. przez pożar, gdy komunikaty nie docierają do łóżka pacjenta personel jest w stanie poinformować o planowanych działaniach

- przekierowywanie przywołań na kolejne oddziały (eskalacja przywołań) bezzwłocznie lub z ustaloną zwłoką czasową z funkcją komunikacji głosowej i akceptacji (indywidualnie dla przywołań pielęgniarskich i indywidualnie dla przywołań lekarskich) – przekierowywanie przywołań musi zostać potwierdzona z inwestorem na etapie programowania,
- przekierowywanie przywołań na telefony (eskalacja przywołań) bezzwłocznie lub z ustaloną zwłoką czasową z funkcją komunikacji głosowej i akceptacji – przekierowywanie przywołań musi zostać potwierdzona z inwestorem na etapie programowania,
- łączenie różnych oddziałów w jeden system z poziomu terminali oddziałowych w punktach pielęgniarskich, funkcja może mieć istotne znaczenie w przypadku absencji personelu lub zmiany organizacji oddziałów bez ingerencji w oprzewodowanie (dostępność łączonych oddziałów musi zostać potwierdzona z inwestorem na etapie programowania),
- urządzenia systemu przyzywowego muszą być podłączane do certyfikowanych systemowych przełączników sieciowych zgodnie z normą DIN VDE 0834,
- urządzenia pracujące na magistrali danych mają być wyposażone w izolatory zwarć a magistrala ma być zasilana dwustronnie w celu zapewnienia najwyższego poziomu bezpieczeństwa w przypadku uszkodzenia pojedynczych urządzeń lub zwarcia przewodów,
- wszystkie urządzenia systemu przyzywowego mają być zasilane napięciem bezpiecznym do 30V DC i ze względów bezpieczeństwa odseparowane galwanicznie od innych instalacji a także przełączników sieci budynkowej,
- system posiada funkcję autodiagnostyki i pokazuje wszystkie informacje o uszkodzonych urządzeniach, modułach lampowych, utracie komunikacji z systemem telefonicznym na wyświetlaczu terminala w dyżurce,
- wszystkie gniazda urządzeń systemu przyzywowego są wyposażone w mechanizm automatycznego wypięcia się wtyczki, chroniącego wtyczkę i gniazdo przed zniszczeniem, zapewniając tym samym zmniejszenie kosztów serwisowych – wypięcie wtyczki urządzenia przyzywowego musi wygenerować alarm przywoławczy personelu pielęgniarskiego z dodatkową informacją o wyciagnięciu wtyczki,
- moduły gniazdowe systemu przyzywowego, do których są podłączane terminale pacjenta z funkcją komunikacji głosowej zapewniają możliwość korzystania z przewodowego Internetu pacjentom (w celu w/w zapewnienia funkcjonalności dopuszcza się zastosowanie oddzielnych, dodatkowych modułów gniazdkowych),
- wszystkie gniazda urządzeń systemu przyzywowego są wyposażone w gniazdo do podłączenia urządzeń medycznych (w celu w/w zapewnienia funkcjonalności dopuszcza się zastosowanie oddzielnych modułów gniazdkowych przy każdym łóżku),
- wyzwalanie przywołań przez pacjentów, personel pielęgniarski lub lekarski w każdym pomieszczeniu uwzględnionym w projekcie,
- wszystkie przywołania są widoczne w obszarze danego oddziału (na wyświetlaczach terminali pokojowych i oddziałowych) lub na oddziałach wzajemnie połączonych,

- wskazania przywołań następują automatycznie według ustawionych w systemie priorytetów, począwszy od największego zgodnie z normą DIN VDE 0834,
- informacja pokazana na wyświetlaczach zawiera następujące informacje:
  - rodzaj przywołania,
  - nazwa pomieszczenia (zgodna z wymaganiami inwestora, minimum 16 znaków z uwzględnieniem znaków polskich),
  - miejsce przywołania np. łóżko lub WC,
- lampki sygnalizacyjne 5 kolorowe wskazujące indywidualnie:
  - 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,
  - kolor żółty – obecność personelu pomocniczego i w pomieszczeniu,
- integrację z centralami telefonicznymi w standardzie SIP, H323 z funkcją prowadzenia rozmów, akceptowania przywołań i pokazywania komunikatów z systemu przyzywowego na wyświetlaczach telefonów,
- system sygnalizacji pożarowej i przyzywowy muszą zostać zintegrowane poprzez protokół cyfrowy zapewniając elastyczność konfiguracji i przekazywanie informacji o pożarze z dokładnością do elementu detekcyjnego w grupie – funkcja udostępnia informację o pożarze personelowi na wczesnym jego etapie pozwalając przygotować się do akcji ewakuacyjnej,
- odbierania programów radiowych za pomocą terminali pacjentów w sposób dyskretny i głośnomówiący a także za pomocą naściennych terminali komunikacyjnych (w celu zapewnienia funkcji dopuszcza się zastosowanie zewnętrznych odbiorników radiowych zabudowanych w ścianie wszędzie tam gdzie zostały przewidziane terminale komunikacyjne i pacjenta),
- system zapewnia w przyszłości możliwość rozbudowy funkcjonalności bez ingerencji w oprzewodowanie w pomieszczeniach pacjentów i personelu na oddziale o:
  - integrację z serwerami alarmów w standardzie ESPA,
  - integrację z automatyką budynkową w standardzie KNX,
  - podłączenie urządzeń specjalistycznych do terminali przyłóżkowych w standardzie IR np. dla osób sparaliżowanych,
  - podłączenie mat sensorycznych do gniazd przyłóżkowych w salach chorych,
  - podłączenie odbiorników bezprzewodowych urządzeń bezprzewodowych przyzywowych do gniazd przy łóżkowych w salach chorych
  - zarejestrowanie terminala pacjenta przy łóżku jako telefonu w centrali telefonicznej np. w izolatkach
  - podłączenie urządzeń medycznych za pomocą dedykowanych interfejsów cyfrowych Drager Infinity Gateway, Philips Emergin Gateway, GE MMG Gateway, Mindray eGateway, OAP, ESPA lub protokół HL7 i przesyłania tych alarmów na telefony mobilne.

Minimalne wymagania funkcjonalne systemu dla pacjentów na oddziale:

- łatwość odnalezienia przycisku lub terminala pacjenta np. w nocy poprzez przyciski przywoławcze posiadające diody podświetlające przyciski,
- wezwanie pielęgniarki - naciśnięcie czerwonego przycisku oznaczonego piktogramem na terminalu pacjenta lub przycisku gruszkowym przy łóżku intensywnie zapala diodę lub przycisk w kolorze czerwonym wskazując zadziałanie systemu,
- w salach chorych po naciśnięciu przycisku przywoławczego przy łóżku pacjenta możliwość porozmawiania z personelem pielęgniarskim przez terminal komunikacyjny na ścianie,
- w izolatkach po naciśnięciu przycisku przywoławczego przy łóżku pacjenta możliwość porozmawiania z personelem pielęgniarskim w sposób dyskretny przez słuchawkę jak również w sposób głośnomówiący, gdy urządzenie znajduje się w uchwycie (o sposobie odbioru decyduje pacjent w danej chwili)
- ograniczenie rozprzestrzeniania się bakterii poprzez zastosowanie foli antybakteryjnej na terminalach pacjentów i terminalach komunikacyjnych w izolatkach,
- wezwanie personelu pielęgniarskiego przy wypięciu się wtyczki przycisku gruszkowego z gniazda np. przy pociągnięciu za kabel (silne pociągnięcie przewodu od przycisku gruszkowego/ terminala pacjenta przy łóżku nie może uszkadzać wtyczki ani gniazda), gniazda są wyposażone w funkcję automatycznego wypinania wtyczek – przywołanie personelu pielęgniarskiego będzie zawierało informacje o wypięciu się wtyczki,
- przywołanie personelu pielęgniarskiego z toalet - naciśnięcie przycisku intensywnie zapala diodę lub podświetla przycisk w kolorze czerwonym, wskazując zadziałanie systemu, przyciski w stanie czuwania są podświetlone w celu łatwej lokalizacji urządzeń,
- linka przycisków pociąganych wraz z systemem mocowań ulega zerwaniu przy maks. sile zrywającej 120N (odpowiadającej wadze ok. 12 kg), w celu ograniczenia możliwości zrobienia sobie krzywdy przez pacjenta,
- gniado Internetowe w zakresie systemu przyzywowego przy każdym łóżku z terminalem pacjenta,
- w izolatkach słuchawki przy łózkach z funkcją komunikacji głosowej mają pracować jako telefony (bez prowadzenia dodatkowego okablowania i ingerencji w instalacje) zalogowane w centrali telefonicznej – funkcjonalność zapewni możliwość dzwonienia do pacjenta przez personel wyposażony w telefony przenośne lub osoby z rodziny, dodatkowo słuchawki nie mogą zawierać szpar pomiędzy przyciskami i muszą być pokryte folią antybakteryjną w celu łatwego czyszczenia urządzeń (licencje do logowania zewnętrznych telefonów musi przewidzieć dostawca centrali telefonicznej)
- słuchanie radia za pomocą terminala pacjenta, terminala komunikacyjnego - komunikaty nadawane przez personel wyciszają automatycznie programy radiowe
- sterowanie 2 źródłami oświetlenia przy łóżku pacjenta za pomocą urządzeń systemu przyzywowego tj. przyłóżkowe przyciski gruszkowe lub terminale pacjentów.

Minimalne wymagania funkcjonalne systemu dla personelu pielęgniarskiego i lekarskiego:

- tekstowe, akustyczne i optyczne sygnalizowanie wszystkich przywołań na terminalach komunikacyjnych, oddziałowych i telefonach medycznych,
- wybór pomieszczenia / łóżka w izolatkach z terminala oddziałowego w punkcie pielęgniarskim i prowadzenia bezpośredniej rozmowy,

- wybór pomieszczenia / łóżka w izolatkach na terminalu oddziałowym w punkcie pielęgniarskim i nasłuchiwania wybranego pomieszczenia (do uzgodnienia z inwestorem),
- zmiana priorytetu przywołania z łóżka na terminalu oddziałowym w punkcie pielęgniarskim – funkcja istotna w przypadku pacjentów bardzie chorych, których przywołania mają być wcześniej widoczne niż innych
- wizualizacja na terminalu oddziałowym w punkcie pielęgniarskim: przywołań, obecności personelu pielęgniarskiego, lekarskiego i pomocniczego w pokojach, przywołań zaakceptowanych z funkcją zapalenia lampki nad drzwiami pokoju do którego udaje się personel,
- wizualizację stanu pracy urządzeń (informacje o uszkodzeniach) na terminalu oddziałowym w punkcie pielęgniarskim,
- optyczne (za pomocą 4 lub 5 kolorowych lampek) sygnalizowanie obecności personelu we wszystkich pomieszczeniach,
- optyczne (za pomocą 4 lub 5 kolorowych lampek) sygnalizowanie przywołań personelu z pomieszczeń,
- odbieranie przywołań i odczytywanie komunikatów tekstowych na wyświetlaczach urządzeń przez personel znajdujący się w dowolnym pomieszczeniu (przewidzianym w projekcie) – funkcja jest dostępna po zaznaczeniu obecności przez personel,
- komunikację głosową pomiędzy personelem pielęgniarskiemu a pacjentem,
- wzajemną komunikację głosową personelu lekarskiego i personelu pielęgniarskiego w pomieszczeniach wyposażonych w terminale komunikacyjne i oddziałowe
- odbieranie przywołań, odczytywanie wszystkich komunikatów tekstowych na wyświetlaczach urządzeń przez personel znajdujący się w dyżurce – funkcja jest dostępna cały czas bez dodatkowych czynności,
- odbieranie przywołań, odczytywanie wszystkich komunikatów tekstowych na wyświetlaczach terminali komunikacyjnych przez personel znajdujący się w salach chorych lub gabinetach – funkcja jest dostępna po zaznaczeniu obecności na terminalu przez personel lub cały czas bez dodatkowych czynności (funkcjonalność zależy od ustaleń z inwestorem),
- komunikacja głosowa w dyżurce musi być dostępna zarówno w sposób dyskretny przez słuchawkę jak również w sposób głośnomówiący (o sposobie odbioru decyduje pielęgniarka), w salach chorych / gabinetach komunikacja głosowa ma odbywać się w sposób głośnomówiący za pomocą terminali komunikacyjnych zainstalowanych na ścianie,
- odbieranie przywołań na telefonach VoIP/DECT posiadanych przez personel medyczny z funkcją:
  - odczytywania komunikatów tekstowych na wyświetlaczach urządzeń,
  - odbierania połączeń,
  - zdalnego kasowania przywołań po rozmowie,
  - zaakceptowania przywołania (przełączania obecności) z funkcją zapalenia lampki w pokoju do którego udaje się personel i przypomnienia w przypadku niepojawienia się w Sali.
- funkcją włączenia lampki nad drzwiami pokoju, z którego nastąpiło przywołanie w celu wydelegowania personelu do pokoju przy odbieraniu przywołań na terminalach komunikacyjnych w salach, oddziałowych w dyżurkach, telefonach mobilnych
- przywołanie personelu pomocniczego z sal chorych,

- przywołanie personelu lekarskiego do pomieszczeń wyposażonych w terminale oddziałowe, komunikacyjne i pokojowe, tzn. sal chorych, pomieszczeń personelu itp
- przywołanie całego zespołu (alarm krytyczny) do pomieszczeń wyposażonych w terminale komunikacyjne i oddziałowe zgodnie z projektem, tzn. sal chorych, pomieszczeń personelu itp
- przywoływanie personelu pielęgniarskiego z opóźnieniem czasowym do sali – alarm ustawiany przez personel pielęgniarski na terminalu komunikacyjnym w sali chorych; alarm ten zostanie uruchomiony automatycznie po ustawionym czasie np. w celu przypomnienia personelowi np. o odłączeniu kroplówki, dokończeniu jakiejś czynności,
- kasowanie przywołań za pomocą terminali komunikacyjnych w pomieszczeniach lub oddzielnych przycisków kasujących,
- kasowanie przywołań bezpośrednio przy łóżku pacjenta w salach chorych i z bezpośrednim nadzorem pielęgniarskim, z wyłączeniem izolatek gdzie przy łózkach zostaną zamontowane terminale z funkcją rozmowy i wbudowanym aparatem telefonicznym SIP
- możliwość kasowania przywołania za pomocą telefonów posiadanych przez personel medyczny po przeprowadzeniu rozmowy,
- ogłaszanie komunikatów głosowych w ramach oddziału do całego personelu, tylko personelu pielęgniarskiego, tylko personelu lekarskiego, do wszystkich włącznie z pacjentami – funkcjonalność ułatwi grupową komunikację m.in. z pacjentami przy obchodach, wydawaniu posiłków i podczas pożaru,
- automatyczne testowanie prawidłowej pracy wszystkich urządzeń systemu i pokazywanie stanu nieprawidłowej pracy urządzeń na terminalu w punkcie pielęgniarskim,
- podłączanie urządzeń medycznych do gniazd systemu przyzywowego znajdujących się przy łóżkach pacjentów w celu przekazania informacji o alarmie z urządzenia medycznego,
- rejestracja wszystkich zdarzeń dostępna za pomocą przeglądarki internetowej z funkcją zarządzania uprawnieniami,
- automatyczne przekierowanie przywołań do pielęgniarek na wybrane numery telefonów medycznych (bezzwłocznie lub ze zwłoką czasową),
- automatyczne przekierowanie przywołań do lekarzy na wybrane numery telefonów medycznych (bezzwłocznie lub ze zwłoką czasową),
- łączenie oddziałów w grupy automatycznie lub manualnie za pomocą terminala oddziałowego znajdującego się w punkcie pielęgniarskim.

<u>Integracja z systemem sygnalizacji pożarowej</u>

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), w dyżurkach pielęgniarskich i/lub na wyświetlaczach telefonów medycznych przypisanych do danego oddziału.

Dodatkowo system przyzywowy posiada funkcję rozgłaszania komunikatów w celu poinformowania pacjentów o planowanym postępowaniu za pomocą terminali znajdujących się w salach i przy łóżkach pacjentów.

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/WIFI. Za dostawę telefonów medycznych i osprzętu odpowiada zamawiający.

Zastosowane rozwiązanie musi umożliwiać komunikację głosową zarówno w ramach systemu przyzywowego i komunikacji jak również z obsługą przemieszczającą się po obiekcie wyposażoną w telefony medyczne.

Połączenie serwera systemu przyzywowego oraz szpitalnej centrali telefonicznej zostanie wykonane w standardzie SIP lub H323.

Słuchanie radia w pomieszczeniach i przy łóżku pacjenta

System przyzywowy ma gwarantować możliwość słuchania, przełączania min 8 programów radiowych, pogłaśniania i przyciszania dźwięku.

Zastosowane rozwiązanie będzie realizowane za pomocą terminali oddziałowych w punktach pielęgniarskich, terminali komunikacyjnych personelu znajdujących się przy drzwiach wejściowych w salach/pomieszczeniach lub przez terminale komunikacyjne pacjentów znajdujące się przy łóżkach w izolatkach.

Personel będzie miał możliwość słuchania radia bezpośrednio z terminali oddziałowych lub komunikacyjnych. Pacjenci będą mieli możliwość słuchania radia z głośnika znajdującego się z słuchawce terminala pacjenta lub za pomocą słuchawek wpinanych do portu typu jack w słuchawce terminala pacjenta.

Steraming audio kanałów radiowych zostanie zrealizowany za pomocą interfejsu dźwięku podłączonego do zewnętrznej anteny/stacji czołowej.

W celu realizacji w/w funkcji dopuszcza się zastosowane wydzielonych odbiorników radiowych IP przy każdym łóżku w izolatce i w pomieszczeniach, gdzie przewidziano terminale komunikacyjne, terminale pacjentów zgodnie z opisaną powyżej funkcjonalnością.

Wymagane dokumenty

Wymagane dokumenty dla urządzeń systemu przyzywowego. System musi posiadać certyfikat potwierdzający spełnianie w pełnym zakresie normy i przepisów:

- DIN-VDE 0834 : 2000 – instalacje przyzywowe w szpitalach, domach opieki i tym podobnych instytucjach,
- DIN-VDE 0834 : 2016/ część 1 – wymogi dla urządzeń, ich produkcji i pracy w obiektach,
- obowiązuje od 1 kwietnia 2000
- DIN-VDE 0834 :2000 / część 2 – kompatybilność elektromagnetyczna i wymogi środowiskowe,
- deklaracje zgodności,
- potwierdzenie w formie pisemnej integracji systemu przyzywowego i wzajemnej współpracy z systemem sygnalizacji pożarowej przez producenta/producentów obydwu systemów.

Montaż instalacji

- System przyzywowy stanowi instalację bezpieczeństwa połączoną z przełącznikami budynkowymi w sieci VLAN.
- Instalację należy wykonać w teletechnicznych korytach kablowych lub w rurkach PCV montowanych do stropu.
- Połączenia należy wykonać przewodem ekranowanym FUTP kat 5e lub nieekranowanym UTP kat. 5e - zgodnie z dokumentacją producenta.
- Przy instalowaniu elementów należy uwzględnić wytyczne do projektowania określające sposób montażu zawarte w dokumentacji producenta.

Rozmieszczenie urządzeń do uzgodnienia w czasie realizacji.

Urządzenia systemu przyzywowego i komunikacji przewidziane w projekcie

Terminal oddziałowy IP

Miejsce montażu:

- w punktach pielęgniarskich.
- montaż nabiurkowy lub naścienny (do uzgodnienia na etapie montażu z inwestorem)

Minimalne parametry techniczne:

- kolorowy dotykowy wyświetlacz min 7’ z szerokim kątem widzenia,
- telefon IP (wymaga zalogowania w centrali telefonicznej),
- interfejs 100BASE-TX,
- nadzorowanie pracy wszystkich urządzeń systemu przyzywowego na oddziale,
- napięcie bezpieczne do 30 VDC.

Minimalna funkcjonalność:

- wskazanie daty i godziny,
- stałe wskazywanie aktualnej liczby przywołań, przekierowanych obecności (zaakceptowanych przywołań z włączoną lampka nad salą do której uda się personel)) i ewentualnych uszkodzeń,
- przewijanie wyświetlanych komunikatów w przypadku wystąpienia kilku/kilkunastu jednoczesnych przywołań,
- wskazanie wszystkich zaznaczonych i zaakceptowanych przywołań (przekierowanych obecności) zgodnie z normą VDE0834,
- wskazanie zdarzeń przekazanych z zewnętrznych systemów do systemu przyzywowego i komunikacji,
- wskazanie wszystkich przywołań automatycznie według priorytetów, począwszy od najwyższego zgodnie z normą DIN VDE 0834
- odbieranie przywołań i komunikacja głosowa na linii: pacjent ←→ personel pielęgniarski ←→ personel lekarski,
- komunikacja głosowa w sposób dyskretny przez słuchawkę lub głośnomówiący bez podnoszenia słuchawki – o sposobie decyduje personel w momencie rozpoczęcia rozmowy,
- przywoływanie personelu pielęgniarskiego z funkcją komunikacji głosowej
- przywoływanie kolejnej osoby z personelu pielęgniarskiego (asysty) z funkcją komunikacji głosowej
- przywoływanie personelu lekarskiego z funkcją komunikacji głosowej
- przywoływanie całego zespołu (pielęgniarki i lekarze) z funkcją komunikacji głosowej
- wybór pomieszczenia / łóżka i prowadzenia bezpośredniej rozmowy,

- wybór pomieszczenia / łóżka i nasłuchiwania wybranego pomieszczenia (do uzgodnienia z inwestorem),
- zmiana priorytetu przywołania z łóżka,
- łączenie oddziałów w grupy automatycznie lub manualnie za pomocą terminala oddziałowego znajdującego się w punkcie pielęgniarskim,
- włączanie grup opieki,
- praca w trybie zcentralizowanym,
- nadawanie komunikatów (zapowiedzi) dla wszystkich osób na oddziale, tylko dla personelu, tylko dla pielęgniarek, tylko dla lekarzy (słuchanie zapowiedzi możliwe jest w pomieszczeniach z terminalami komunikacyjnymi i terminalami pacjenta),
- terminal wyświetla informacje o prawidłowej pracy systemu (system automatycznie kontroluje stan pracy urządzeń), uszkodzenia systemu/urządzeń wyświetlane są na wyświetlaczu.

Terminal komunikacyjny IP

Miejsce montażu:

- pokoje łóżkowe, pokoje zabiegowe, sale obserwacyjne, sale intensywnego nadzoru, pokoje klasyfikacji, pomieszczenia przyjęć dzieci i kobiet, sale chem, izolatki, sale zabaw, gabinety i pokoje lekarskie, pokoje przygotowania pielęgniarek, dyżurki lekarskie, pom. socjalne i w pozostałych pomieszczeniach zgodnie z projektem
- montaż naścienny.

Minimalne parametry techniczne:

- wyświetlacz graficzny mogący pokazywać teksty minimum 4 linie po 16 znaków,
- obudowa i przyciski z folią antybakteryjną
- interfejs 100BASE-TX dla systemu przywoławczego,
- interfejs 100BASE-TX dla systemu zewnętrznego,
- 9 przycisków funkcyjnych
- 6 diody LED potwierdzające zadziałanie funkcji przycisków
- napięcie bezpieczne do 30 VDC.

Minimalna funkcjonalność:

- wskazanie daty i godziny,
- wskazywanie i odbieranie przywołań,
- przewijanie przyciskami funkcyjnymi wyświetlanych komunikatów w przypadku wystąpienia kilku jednoczesnych przywołań,
- wskazanie zdarzeń przekazanych z zewnętrznych systemów do systemu przyzywowego i komunikacji,
- wskazanie wszystkich przywołań automatycznie według priorytetów, począwszy od najwyższego zgodnie z normą DIN VDE 0834
- odbieranie przywołań i komunikacja głosowa na linii: pacjent ←→ personel pielęgniarski ←→ personel pomocniczy ←→ personel lekarski,
- przywoływanie personelu pielęgniarskiego z funkcją komunikacji głosowej
- przywoływanie kolejnej osoby z personelu pielęgniarskiego (asysty) z funkcją komunikacji głosowej
- przywoływanie personelu lekarskiego z funkcją komunikacji głosowej
- przywoływanie całego zespołu (pielęgniarki i lekarze) z funkcją komunikacji głosowej

- nadawanie komunikatów (zapowiedzi) dla wszystkich osób na oddziale, tylko dla personelu, tylko dla pielęgniarek, tylko dla lekarzy (słuchanie zapowiedzi możliwe jest w pomieszczeniach z terminalami komunikacyjnymi i terminalami pacjenta),
- przywoływanie personelu pielęgniarskiego z opóźnieniem czasowym – alarm ustawiany przez personel pielęgniarski który zostaje uruchomiony po ustawionym na terminali w pokoju czasie np. w celu przypomnienia personelowi o dokończeniu jakiejś czynności.

Terminal pokojowy

Miejsce montażu:

- łazienki, toalety i WC zgodnie z projektem
- montaż naścienny

Minimalne parametry techniczne:

- klawiatura membranowa przeznaczona do obsługi
- przyciski pokryte folią antybakteryjną
- 4 przyciski funkcyjne,
- 4 diody LED potwierdzające zadziałanie funkcji przycisków
- napięcie bezpieczne do 30 VDC,
- dwustronne podłączenie do magistrali danych w kształcie pierścienia ze względu na możliwość zachowania ciągłości pracy podczas pojedynczego uszkodzenia okablowania.

Minimalna funkcjonalność:

- sygnalizowanie zdarzeń przekazanych z zewnętrznych systemów do systemu przyzywowego i komunikacji,
- sygnalizowanie wszystkich przywołań automatycznie według priorytetów, począwszy od najwyższego zgodnie z normą DIN VDE 0834
- odbieranie przywołań na linii:
  - pacjent ←→ personel pielęgniarski
  - personel pielęgniarski ←→ personel pielęgniarski
  - personel pielęgniarski ←→ personel lekarski
  - personel lekarski ←→ personel lekarski
- przywoływanie personelu pielęgniarskiego
- przywoływanie kolejnej osoby z personelu pielęgniarskiego (asysty)
- przywoływanie personelu lekarskiego

Terminal pacjenta IP

Miejsce montażu:

- w izolatkach,
- montaż w uchwytach przy łóżku pacjenta

Minimalne parametry techniczne:

- wyświetlacz graficzny,
- obudowa i przyciski z folią antybakteryjną
- wbudowany switch 100BASE-TX,
- wbudowany, bezdotykowy czytnik kart chip,

- mechaniczne mocowanie karty chip,
- odbiornik podczerwieni służący do podłączenia i odbierania alarmów z urządzeń specjalistycznych,
- kabel przyłączeniowy o długości min. 2,80 m z samoczynnie wypinającą się wtyczką przy pociagnięciu, chroniącą ją przed zniszczeniem, przerwaniem lub wyrwaniem kabla
- napięcie bezpieczne do 30 VDC.

Minimalna funkcjonalność:

- wskazanie daty i godziny,
- przycisk przywoławczy z symbolem pielęgniarki na stronie czołowej z podświetleniem w nocy w celu łatwego odnalezienia i diodą potwierdzającą zadziałanie w celu pokazania zadziałania,
- komunikacja głosowa w sposób dyskretny przez słuchawkę lub głośnomówiący po odłożeni do uchwytu – o sposobie decyduje pacjent,
- przywoływanie personelu pielęgniarskiego z funkcją komunikacji głosowej,
- przywoływanie kolejnej osoby z personelu pielęgniarskiego (asysty) z funkcją komunikacji głosowej – funkcja dostępna dla personelu pielęgniarskiego po zaznaczeniu obecności na terminalu komunikacyjnym w sali,
- przywoływanie personelu pomocniczego np. salowej z funkcją komunikacji głosowej,
- podłączanie urządzeń specjalistycznych za pomocą odbiornika podczerwieni,
- przywołanie dodatkowych osób z personelu zdefiniowanych na etapie programowania.

Moduł gniazdkowy IP

Miejsce montażu:

- w salach chorych, izolatkach,
- montaż naścienny lub w panelach nadłóżkowych.

Minimalne parametry techniczne:

- gniazdo do podłączenia terminali pacjentów IP,
- gniazdo do podłączenia laptopa
- gniazdo diagnostyczne modułu gniazdkowego służące do podłączenia wedle potrzeby: urządzenia medycznego posiadającego alarmowy zestyk bezpotencjałowy, tj. inkubatory, pompy infuzyjne itp.
- wyposażony w mechanizm automatycznego wypięcia się wtyczki, chroniącego wtyczkę przed zniszczeniem.
- napięcie bezpieczne do 30 VDC.

Przycisk gruszkowy

Miejsce montażu:

- w salach obserwacyjnych, salach IT, salach wybudzeń, salach łóżkowych, pokojach. badań, prac. specjalistycznych, gabinetach zabiegowych, pok. klasyfikacji, pom. przyjęć dzieci i kobiet ciężarnych, gab. zabiegowych, pok. przyjęć kobiet ciężarnych, gab. badań KTG, pok. przyjęć dzieci, pok. badań, prac. echo, prac. elektrokardiografii, salach ergospirometrii i pozostałych wrysowanych w projekcie
- montaż w uchwytach przy łóżku pacjenta

Minimalne parametry techniczne:

- kabel przyłączeniowy o długości 2,80 m z wtyczką,
- kabel przyłączeniowy z samoczynnie wypinającą się wtyczką przy pociągnięciu chroniącą przed zniszczeniem wtyczki, przerwaniem lub wyrwaniem kabla
- napięcie bezpieczne do 30 VDC.

Minimalne funkcjonalność:

- przycisk przywoławczy z symbolem pielęgniarki na stronie czołowej z podświetleniem w nocy w celu łatwego odnalezienia i diodą potwierdzającą zadziałanie w celu pokazania zadziałania,
- przywoływanie personelu pielęgniarskiego
- przywoływanie kolejnej osoby z personelu pielęgniarskiego (asysty) z funkcją komunikacji głosowej – funkcja dostępna dla personelu pielęgniarskiego po zaznaczeniu obecności na terminalu komunikacyjnym w sali

Moduł gniazdkowy dla przycisku gruszkowego

Miejsce montażu:

- w salach obserwacyjnych, salach IT, salach wybudzeń, salach łóżkowych, pokojach. badań, prac. specjalistycznych, gabinetach zabiegowych, pok. klasyfikacji, pom. przyjęć dzieci i kobiet ciężarnych, gab. zabiegowych, pok. przyjęć kobiet ciężarnych, gab. badań KTG, pok. przyjęć dzieci, pok. badań, prac. echo, prac. elektrokardiografii, salach ergospirometrii i pozostałych wrysowanych w projekcie
- montaż naścienny lub w panelach nadłóżkowych

Minimalne parametry techniczne:

- do podłączenia przycisków gruszkowych,
- wyposażony w mechanizm automatycznego wypięcia się wtyczki, chroniącego wtyczkę przed zniszczeniem.
- gniazdo diagnostyczne modułu gniazdkowego służące do podłączenia wedle potrzeby: urządzenia medycznego posiadającego alarmowy zestyk bezpotencjałowy, tj. inkubatory, pompy infuzyjne itp.
- napięcie bezpieczne do 30 VDC.

Minimalna funkcjonalność:

- przywoływanie personelu pielęgniarskiego
- kasowanie przywołania bezpośrednio przy łóżku
- podłączanie urządzeń medycznych

Przycisk przywoławczy

Miejsce montażu:

- łazienki, toalety i WC
- montaż naścienny

Minimalne parametry techniczne:

- klawiatura membranowa przeznaczona do obsługi
- 1 przycisk przywoławczy z podświetleniem,
- 1 dioda LED potwierdzająca zadziałanie funkcji przywołania w przycisku

- napięcie bezpieczne do 30 VDC,
- dwustronne podłączenie do magistrali danych w kształcie pierścienia ze względu na możliwość zachowania ciągłości pracy podczas pojedynczego uszkodzenia okablowania.

Minimalna funkcjonalność:

- przywoływanie personelu pielęgniarskiego
- przywoływanie kolejnej osoby z personelu pielęgniarskiego (asysty) z funkcją komunikacji głosowej – funkcja dostępna dla personelu pielęgniarskiego po zaznaczeniu obecności na terminalu komunikacyjnym lub pokojowym

Przycisk przywoławczy pociągany zabezpieczony przed wilgocią

Miejsce montażu:

- łazienki , toalety i WC itp
- montaż naścienny

Minimalne parametry techniczne:

- 1 przycisk przywoławczy pociągany,
- mikroprzełącznik z 2-metrową linką pociągową (maks. siła zrywająca 120N odpowiada ok. 12 kg), z karabinkiem, zakończona uchwytem z symbolem pielęgniarki (ze względów higienicznych uchwyt musi być wymieniany w prosty sposób)
- przywoławczy pociągany zabezpieczony przed wilgocią, IP44
- napięcie bezpieczne do 30 VDC,
- dwustronne podłączenie do magistrali danych w kształcie pierścienia ze względu na możliwość zachowania ciągłości pracy podczas pojedynczego uszkodzenia okablowania.

Minimalna funkcjonalność:

- przywoływanie personelu pielęgniarskiego
- przywoływanie kolejnej osoby z personelu pielęgniarskiego (asysty) z funkcją komunikacji głosowej – funkcja dostępna dla personelu pielęgniarskiego po zaznaczeniu obecności na terminalu komunikacyjnym lub pokojowym

Lampka sygnalizacyjna

Miejsce montażu:

- przy pomieszczeniach od strony ciągów korytarzowych
- montaż naścienny

Minimalne parametry techniczne:

- 5 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 jaskrawożółte diody LED,
- 1 komory wyposażonej w 3 świecące jaskrawoniebieskie diody LED,
- każda komora oświetleniowa spełnia wymagania natężenia światła zgodnie z VDE0834,
- diody LED o żywotności około 100.000 roboczogodzin

- napięcie bezpieczne do 30 VDC,
- dwustronne podłączenie do magistrali danych w kształcie pierścienia ze względu na możliwość zachowania ciągłości pracy podczas pojedynczego uszkodzenia okablowania.

Minimalna funkcjonalność:

- możliwość oprogramowania jako lampki pokojowej, kierunkowej lub grupowej
- znaczenie kolorów:
  - 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,
  - kolor żółty –obecność personelu pomocniczego w pomieszczeniu,

Interfejs dźwięku

Miejsce montażu:

- w pomieszczeniu technicznym przy stacji antenowej/stacji czołowej
- montaż naścienny

Minimalne parametry techniczne:

- montaż naścienny lub w szafie RACK
- zasilanie 230VAC
- budowa modułowa

Minimalna funkcjonalność:

- Interfejs dźwięku jest przeznaczony do odbioru do 16 programów radiowych i ich konwersji na sygnał cyfrowy.
- Programy radiowe wysyłane są do sieci komunikacyjnej jako tzw. audiostreams poprzez switch systemowy. Zintegrowane w poszczególnych modułach tunery UKF przeznaczone są dla zakresu od 87,5 do 108.0 MHz z funkcją automatycznego dostrojenia.
- Ponadto interfejs dźwięku umożliwia przekonwertowanie sygnałów częstotliwości akustycznej wygenerowanych z systemów zewnętrznych na sygnał cyfrowy i za pomocą transmisji strumieniowej rozesłany poprzez sieć. Sygnały częstotliwości akustycznej tego typu mogą mieść nadany charakter „obowiązkowego odbioru“ i mogą zostać podzielone według priorytetów.

Instalacja okablowania

Wzdłuż głównych ciągów komunikacyjnych przewiduje się układanie przewodów w korytkach metalowych nad sufitem podwieszanym równolegle z pozostałymi instalacjami teletechnicznymi. Przy odejściach od głównych tras kablowych do poszczególnych pomieszczeń okablowanie należy układać w rurkach elektroinstalacyjnych natynkowo (nad

sufitem podwieszanym) lub w korytkach kablowych o szerokości 50mm (nad sufitem podwieszanym) lub podtynkowo (na odejściach od przestrzeni nad sufitem podwieszanym do gniazd lub urządzeń końcowych).

5.13 System AV

Zawartość

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.

Założenia programowe i funkcjonalne

Główne założenia programowe i funkcjonalne:

- wyświetlanie prezentacji multimedialnych,
- nagłośnienie prezentacji multimedialnych,
- sterowanie wyposażeniem multimedialnym,
- sterowanie oświetleniem,
- sterowanie zaciemnieniem.

System Zarządzania powinien umożliwiać kompleksowe zarządzanie wszystkimi systemami składowymi, prowadzenie konferencji, prezentacji multimedialnych, szkoleń itp. Powinien zapewniać łatwość obsługi i dostosowania systemów zgodnie z wymogami Użytkownika, oferować rozwiązania praktycznie zweryfikowane w realizacjach podobnych obiektów o wysokim standardzie wyposażenia oraz możliwość nadzoru i zarządzania wyposażeniem multimedialnym. Wymagana jest spójność i wysoka niezawodność systemu dlatego system dystrybucji sygnałów AV wraz z systemem sterowania powinna być jednego producenta.

Elementy systemu

Standard 1

W pomieszczeniu na ścianie zostanie zainstalowany za pomocą dedykowanego uchwytu ściennego monitor 85”

Monitor zostanie podłączony: do zasilania 230V, sieci LAN budynkowej oraz do odbiornika transmisji sygnałowej AV za pomocą kabla HDMI (zainstalowany na plecach monitora).

W biurku zostanie zainstalowane przyłącze stołowe (mediabox) wyposażone w wejścia AV HDMI oraz VGA, audio. Okablowanie z przyłącza zostanie podłączone do nadajnika AV zamontowanego pod blatem (lub w dedykowanym miejscu np. półka, szafka). Z nadajnika za pomocą patchcorda łączymy się do przyłącza ściennego skąd dalej transmisja idzie do odbiornika zlokalizowanego na plecach monitora.

Standard 2

W pomieszczeniu na ścianie zostanie zainstalowany za pomocą dedykowanego uchwytu ściennego monitor 85”.

Monitor zostanie podłączony: do zasilania 230V, sieci LAN budynkowej oraz do odbiornika transmisji sygnałowej AV za pomocą kabla HDMI (zainstalowany na plecach monitora).

Z odbiornika zostanie wydzielony sygnał audio doprowadzony zestawu kolumn aktywnych zainstalowanych także na ścianie przedniej.

W biurku zostanie zainstalowane przyłącze stołowe (mediabox) wyposażone w wejścia AV HDMI oraz VGA, audio. Okablowanie z przyłącza zostanie podłączone do nadajnika AV zamontowanego pod blatem (lub w dedykowanym miejscu np. półka, szafka). Z nadajnika za pomocą patchcorda łączymy się do przyłącza ściennego skąd dalej transmisja idzie do odbiornika zlokalizowanego na plecach monitora.

Ponadto w blacie biurka zostanie zainstalowany panel sterujący umożliwiający zarządzaniem sygnałami audio i video. W ramach biurka należy zainstalować niezbędne elementy do poprawnego działania systemu m.in. switch, zasilacz, konwerter.

Standard 3

W pomieszczeniu na ścianie zostanie zainstalowany za pomocą dedykowanego uchwytu ściennego monitor 75".

Monitor zostanie podłączony: do zasilania 230V, sieci LAN budynkowej oraz do odbiornika transmisji sygnałowej AV za pomocą kabla HDMI (zainstalowany na plecach monitora).

Z odbiornika zostanie wydzielony sygnał audio doprowadzony zestawu kolumn aktywnych zainstalowanych także na ścianie przedniej.

Na ścianie zostanie zainstalowane przyłącze wyposażone w wejścia AV 1xHDMI oraz 1xVGA, audio (nadajnik aktywny). Z nadajnika dalej transmisja idzie do odbiornika zlokalizowanego na plecach monitora.

Powyżej podtynkowo zostanie zainstalowany panel sterujący umożliwiający zarządzaniem sygnałami audio i video.

Ponadto nad sufitem należy zainstalować niezbędne elementy do poprawnego działania systemu m.in. switch, zasilacz, konwerter.

Standard 4

System wizyjny:

Na system wizyjny składają się 3 projektory - charakteryzuje się jasnością wynoszącą 6000 lumenów oraz rozdzielczością FullHD. Niezwykle ostry obraz oraz wysokie natężenie światła białego i barwnego sprawiają, że prezentacje wyglądają wyraziście i czytelnie nawet w mocno nasłonecznionych pomieszczeniach. Model to projektor laserowy dzięki czemu urządzenie może pracować praktycznie bez żadnej konserwacji nawet przez 20 000 godzin. Nie ma też ryzyka niespodziewanej awarii lampy, kosztów ich zakupu oraz wymiany. Projektor jest objęty gwarancją na 5 lat lub 12 000 godzin.

Projektor zostanie zamocowany na solidnym uchwycie sufitowym zapewniającym stabilność, bez ryzyka jakiegokolwiek uszkodzenia.

Obraz z projektora wyświetlany będzie na 3 ekranach elektrycznych zamontowanych na trzech różnych ścianach. Zastosowany materiał projekcyjny pozwala uzyskać szeroki kąt widzenia, wysoką jasność i doskonałe właściwości rozpraszania światła, jednolitość koloru, dla zwiększenia kontrastu oraz efektu wizualnego ekranu zastosowane zostały czarne ramki.

System dystrybucji sygnału:

Sygnał przesyłany jest poprzez przyłącza ścienne zlokalizowane w pobliży ekranów projekcyjnych. Przyłącze wyposażone jest w gniazdo HDMI, VGA, Audio oraz LAN. Zastosowanie standardów cyfrowych oraz analogowych daje możliwość podłączenia praktycznie każdego źródła sygnału.

Sercem systemu jest jednostka centralna umożliwiająca pełną kontrolę prezentacji i przełączanie sygnału. Integracja systemu sterowania pozwala na sterowanie wszystkimi urządzeniami systemu AV, zaciemnieniem oraz światłem wł/wył. z jednego miejsca sali. Multimedialna krosownica pozwala na stworzenie kilku punktów przyłączeniowych, przyjęcie wielu oraz wypuszczenie jednego lub wielu wskazanych przez użytkownika sygnałów wizyjnych do projektorów . Funkcja skalowania pozwala na przyjęcie wszystkich możliwych rozdzielczości i skaluje je do jednej natywnej rozdzielczości projektora tj. 1920x1200 (FullHD). Oznacza to że prelegent nie musi martwić się ustawieniami laptopa, po włożeniu wtyczki HDMI do przyłącza - procesor zawsze wyświetli obraz na projektorze z pełnym wykorzystaniem ekranu. Wbudowany deembeder samoistnie wydzieli sygnał Audio z aktywnego źródła HDMI i wypuści dźwięk na głośniki.

System nagłośnienia:

Dźwięk realizowany jest poprzez wysokiej klasy 20-watowe głośniki sufitowe. Głośnik ten to model nadający się doskonale do odtwarzania mowy przez mikrofon oraz czysty dźwięk dla wszystkich aplikacji muzycznych.

System mikrofonów zawiera cztery bezprzewodowe mikrofony doręczne oraz dwa mikrofony nagłowne. Mikrofony posiadają bardzo funkcjonalną kardioidalną charakterystykę kierunkowości co powoduje odbiór dźwięków dochodzących z przodu mikrofonu oraz nieznacznej ilości dźwięków z jego boków i został zaprojektowany w celu uzyskania ciepłego i czystego brzmienia. System charakteryzuje się niezwykle łatwą obsługą oraz wysoką niezawodnością. Jego zasięg to około 90m.

Dla poprawności odbioru sygnału z nadajników mikrofonowych zastosowano zewnętrzne anteny zbierające sygnał.

Jako końcówki mocy zastosowany zostały 2 wzmacniacze klasy D w technologii 100V

System sterowania:

System sterowania składa się z ściennego 7 calowego panela dotykowego zlokalizowanego przy głównym ekranie oraz mobilnego panela dotykowego. Zastosowanie paneli dotykowych pozwala na stworzenie spersonalizowanej szaty graficznej poczynając od zaprojektowania przycisków o dowolnej funkcjonalności kończąc na umieszczeniu loga placówki. Panel dotykowy skonfigurowany zostanie tak aby jednym kliknięciem włączyć projektor, opuścić ekran, wyświetlić domyślny sygnał video. Pozwala również na przełączanie źródeł wideo oraz regulację głośności.

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).

Przy drzwiach zostaną zainstalowane klawiatury sterujące które będą wywoływały zaprogramowaną scenę świetlna.

Cały sprzęt zostanie zamknięty w szafie RACK 19".

System centralnego sterowania wszystkimi salami AV

W ramach inwestycji zaprojektowano montaż jednostki centralnej w pomieszczeniu teletechnicznym i wpięcie jej do sieci budynkowej. Na potrzeby systemu należy wydzielić niezależną sieć V-LAN.

Za pomocą dedykowanego monitora dotykowego będzie możliwość zarządzania i nadzoru nad urządzeniami w systemie (monitor musi pracować w tej samej sieci!). technik bez ruszania się z miejsca będzie miał nadzór urządzeniami oraz możliwość zdalnego wsparcia w celu rozwiązania ewentualnych problemów.

Panel zostanie graficznie i funkcjonalnie spersonalizowany indywidualnie do potrzeb systemu.

ZESTAWIENIE URZĄDZEŃ

Lp	ID Urządzenia	Nazwa	Ilość
		STANDARD 1	
1	01	Monitor	1
2	02	Uchwyt do monitora	1
3	03	Zestaw transmisji	1
4	04	Przyłącze stołowe (mediabox)	1
5		Okablowanie	1
6		Zaprogramowanie	1
7		Montaż, uruchomienie, testowanie	1
		Standard 2	
1	01	Monitor	1
2	02	Uchwyt do monitora	1
3	03	Zestaw transmisji	1
4	04	Przyłącze stołowe (mediabox)	1
5	05	Zestaw kolumn aktywnych	1
6	06	Panel sterujący	1
7	07	Konwerter IP/RS232	1

8	08	Switch	1
9	09	Zasilacz Poe	1
10		Okablowanie	1
11		Zaprogramowanie	1
12		Montaż, uruchomienie, testowanie	1
		Standard 3	
1	01	Monitor	1
2	02	Uchwyt do monitora	1
3	03	Zestaw transmisji ścienny	1
4	04	Przyłącze stołowe (mediabox)	1
5	05	Zestaw kolumn aktywnych	1
6	06	Panel sterujący	1
7	07	Konwerter IP/RS232	1
8	08	Switch 8 portowy	1
9	09	Zasilacz Poe	1
10		Okablowanie	1
11		Zaprogramowanie	1
12		Montaż, uruchomienie, testowanie	1
		Standard 4	
		System wizyjny	
1	01	Projektor laserowy	3
2	02	Uchwyt do projektora	3
3	03	Ekran elektryczny	3
4	04	Przyłącze ścienne AV	3
5	05	Odbiornik sygnałowy	1
6	06	Nadajnik sygnałowy	1
7	07	Odbiornik sygnałowy ze skalerem	3
		System audio	
8	08	Mikrofon bezprzewodowy do ręki	4

9	09	Mikrofon bezprzewodowy nagłowny	2
10	10	Splitter wzmacniacz antenowy	2
11	11	Zewnętrzna antena	2
12	12	Akumulator	6
13	13	Ładowarka do akumulatorów	3
14	14	Wzmacniacz mocy 120W/100V	2
15	15	Kolumna sufitowa wpuszczana	4
		System centralnego sterowania i matrycowania	
16	16	Jednostka centralna	1
17	17	Zasilacz systemowy 1	1
18	18	Dotykowy panel sterujący 7"	1
19	19	Puszka podtynkowa panela	1
20	20	Zasilacz Poe	1
21	21	Panel dotykowy sterujący bezprzewodowy	1
22	22	Klawiatura sterująca (przy drzwiach)	3
23	23	Moduł sterowania oświetleniem DALI	1
24	24	Moduł sterowania silnikami	1
25	25	Zasilacz systemowy 2	1
		Pozostałe	
26	26	Acces point	1
27	27	Router	1
28	28	Szafa rack z akcesoriami	1
29		Okablowanie	1
30		Zaprogramowanie	1
31		Montaż, uruchomienie, testowanie	1

		Centrum zarządzania	
1		Jednostka centralna	1
2		Panel sterujący	1
3		Zaprogramowanie	1
4		Montaż, uruchomienie, testowanie	1

Standardy wyposażania

Budynek	Kondygnacja	nazwa pomieszczenia	numer	proponowany standard
A1	P0	Sala studentów	P0.CJD.12	standard 1
	P1	Sala seminaryjna	P1.CN.16	standard 1
	P3	Sala seminaryjna	P3.RAD.20	standard 1
	P4	Sala seminaryjna	P4.KD.1	standard 1
	P5	Sala seminaryjna	P5.EK.17	standard 1
	P7	Sala seminaryjna	P7.UR.47	standard 1
	P8	Sala seminaryjna	P8.MP.7	standard 1
	P10	Sala seminaryjna	P10.CO.13	standard 1
		Sala seminaryjna	P10.CO.100	standard 1
		Sala seminaryjna	P10.CO.90	standard 1
	P11	Sala seminaryjna	P11.GE.12	standard 1
		Sala seminaryjna	P11.NR.32	standard 2
		Sala seminaryjna	P11.NR.33	standard 2
	P12	Sala szkoleniowo-debryfingowa	P12.SM.1	standard 3
		Sala szkoleniowo-debryfingowa	P12.SM.2	standard 3
		Sala szkoleniowo-debryfingowa	P12.SM.3	standard 3
		Sala szkoleniowo-debryfingowa	P12.SM.4	standard 3
		Sala szkoleniowo-debryfingowa	P12.SM.5	standard 3
		Sala szkoleniowo-debryfingowa	P12.SM.6	standard 3
	P14	Sala seminaryjna	P14.PiO.58	standard 2
		Sala seminaryjna	P14.PiO.61	standard 1
		Sala seminaryjna	P14.PH.31	standard 2
	P15	Sala seminaryjna	P15.CH.54	standard 3
		Sala seminaryjna	P15.CH.55	standard 2
		Sala seminaryjna	P15.ENK.1	standard 1
	P16	Sala seminaryjna	P16.PO.2	standard 1
		Sala seminaryjna	P16.NN.12	standard 1

A2	P02	Sala seminaryjna	P02.LD.12	standard 3
	P01	Sala seminaryjna	P01.END.43	standard 3
		Sala seminaryjna	P01.SN.8	standard 3
		Sala seminaryjna	P01.SN.13	standard 3
	P0	Sala seminaryjna	P00.ADM.1	standard 4
		Sala seminaryjna	P00.COK.1	standard 3
	P1	Sala szkoleniowa	P1.ADM.101	standard 3
		Sala seminaryjna	P1.ADM.44	standard 2
		Sala seminaryjna	P1.ADM.16	standard 3
		Sala konferencyjna	P1.BR.17	standard 3
		Sala konferencyjna	P1.BR.18	standard 3
		Sala konferencyjna	P1.BR.11	standard 3
		Sala szkoleniowa	P1.AP.5	standard 2

Zaznaczone na szaro pomieszczenia poza zakresem niniejszego opracowania.

Parametry minimalne urządzeń

Monitor:

- Jasność min. 350 cd/m2
- Rozdzielczość min. 3840 x 2160 (UHD)
- Kontrast typowy: 1400:1
- Przekątna min. 74”-76”
- Waga: max. 34,6 kg
- Oprogramowanie zarządzające treścią
- Złącza: min. 1x RJ45, min. 1x RS232C
- Wejścia: min. 3x HDMI, min. 1x USB
- Wyjścia: min. 1x optyczne, min. 2x Audio, min. 1x słuchawkowe
- Tryb pracy ciągłej min. 16 godzin
- Funkcja bezprzewodowego Acces Pointu
- Certyfikacja Crestron Connected®
- Funkcja BLE (Bluetooth Low Energy)
- Wbudowane głośniki min. 2x 10W

Uchwyt do monitora:

- Uchwyt dopasowany do rozmiaru oferowanego monitora
- Odległość od ściany: min.13cm
- Standard VESA max. 1000:800
- Udźwig min. 125 kg
- Pochył min. 30^{o} ($-15^{o}/+15^{o}$ przód/tył)
- Gwarancja min. 5 lat

Zestaw transmisji:

- Nadajnik typu box z wbudowanym automatycznym switcherem
- Auto detekcja podłączonego źródła
- Wbudowany scaler sygnałowy do rozdzielczości 1920x1200
- Wejście 2xHDMI, VGA audio, Ethernet
- Odbiornik posiadający wejście HDMI, wyjście HDMI, wyjście audio(wydzielenie z HDMI), RS232, IR, Ethernet
- Transmisja na min 70m, konfiguracja i obsługa poprzez przeglądarkę internetową

Przyłącze stołowe:
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

Zestaw kolumn aktywnych:

- Moc min. 2x 15W RMS
- Moc szczytowa min. 2x 30W
- Wielkość głośnika niskotonowego mi. 5,25”

- Wielkość głośnika wysokotonowego min 1”
- Dwudrożna konstrukcja
- Waga max. 5.6 kg
- Dyspersja horyzontalna/wertykalna: $180^{o}/180^{o}$
- Maksymalne SPL 1m min.101 dB
- Pasmo przenoszenia min. 45 -20000 Hz
- Stopień ochrony IP: min. 40

Panel sterujący:

- Możliwość regulacji dźwięku przycisków
- Automatyczna kontrola jasności
- Min. 6 konfigurowalnych przycisków z wymiennymi ikonami
- Aplikacja sterująca kompatybilna z Android, Ios
- Wsparcie zdalnego zarządzania SNMP
- Wsparcie języków Unicode
- Wsparcie protokołów TLS, SSL, SSH, SFTP
- Dostosowany do IPv6
- Czujnik bliskości
- Dodatkowe przyciski stanu włączenia, wyciszenia, regulacji głośności oraz wskaźnik poziomu głośności
- Złącze LAN PoE,

Konwerter IP/RS232:

- Możliwość montażu na ścianie lub szynie DIN
- Diody LED ułatwiające diagnozowanie sieci
- Przycisk Reset przywracający ustawienia fabryczne
- Interfejs Ethernet zgodny z IEEE 802.3, IEEE 802.3u 10/100Base-TX
- Obsługa auto MDI/MDI-X na porcie RJ-45
- 1x port RS-232 / 422 / 485 oraz jeden 10/100Base-TX
- Obsługa RS-232, 4-przewodowego RS-422 oraz 2/4-przewodowego RS-485
- Asynchroniczne przesyłanie danych z prędkością min. 921600b/s
- Aktualizacja oprogramowania Firmware poprzez http
- Programowa obsługa protokołów ARP, ICMP,TCP / IP, UDP, HTTP server, DHCP client, Telnet server/client
- Wbudowany interfejs sieciowy oparty na IP do zdalnego zarządzania
- Tryb połączenia w parze umożliwiający połączenie dwóch urządzeń z interfejsem szeregowym poprzez sieć

Switch:

- Automatyczna negocjacja szybkości połączeń i automatyczne krosowanie
- Wydajność przełączania min. 16Gb/s
- Rozmiar bufora : min 2Mb
- Tablica adresów MAC : 8K
- Szybkość przekierowań pakietów min. 11,9Mp/s
- Obsługa protokołów: IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab , IEEE 802.3x
- 8 portów RJ45 10/100/1000Mb/s

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

Zestaw transmisji 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

Switch 8 portowy:

- Porty: min. 8 x 10/100/1000Mb/s
- Rozmiar bufora: 2Mb
- Przepustowość wewnętrzna: 16Gb/s
- Tablica adresów MAC: 8000
- Standardy: 802.3/u/ab/x, TCP/IP

Projektor laserowy:

- technologia - 3LCD;
- natężenie światła - min. 6000 lumenów;
- rozdzielczość - WUXGA (1920 x 1200);
- współczynnik proporcji - 16:10;
- stosunek kontrastu - min 2.000.000 : 1;
- źródło światła - laser, żywotność min. 20 000 h;
- korekcja Lens-Shift;
- przystosowany do pracy 24 h / 7 dni;
- montaż projektora w dowolnej pozycji (360 stopni);
- poziom hałasu w trybie normalnym maks. 40db;
- wejścia: 2 x VGA, HDBaseT, 2x HDMI, 2x Audio mini jack, RS-232, LAN;
- wyjścia: VGA, Audio mini jack;
- wysłona złączy i okablowania dostarczana w komplecie razem z projektorem;
- szybki start i wyłączenie;
- kolor obudowy biały.

Uchwyt do projektora:

- 4 punkty mocowania
- Blacha o grubości 3 mm malowana proszkowo
- Teleskopowa konstrukcja uchwytu o profilu okrągłym
- Możliwość regulacji min. 62-84 cm
- Korekta lewo/prawo 18°/18°
- Regulacja kąta nachylenia 90°/90°
- Prowadzenie okablowania wewnątrz uchwytu
- malowany proszkowo na kolor biały

Ekran elektryczny:

- obszar roboczy min. 233 cm x 145,6 cm

- płótno z czarnym tyłem
- czarne ramki (wykonane z płótna, nie dopuszcza się malowanych ramek)
- format 16:10,
- wysuw płótna przedni,
- kolor kasety biały,
- płótno posiada certyfikat trudnopalności,
- boczki ekranu wykonane z aluminium

Przyłącze ścienne AV:

Urządzenie transmitujące sygnał AV po skrętce na odległość 100m, przeznaczone do zabudowy ściennej.

- Wbudowany automatyczny switcher
- Złącza na wyposażeniu:
- - 1 x wejście USB HID
- - 1 x wyjście RJ-45 obsługujące transmisję sygnału po skrętce
- - 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
- Czarny kolor ramki ściennej

Odbiornik sygnałowy:

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

Nadajnik sygnałowy:

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 sygnałowy ze skalerem:

- Odbiornik cyfrowego sygnału HDBaseT

- Wyjście HDMI
- Wbudowany scaler video obsługujący rozdzielczości WUXGA
- Port dwukierunkowy RS-232, IR, Ethernet, USB HID

Mikrofon bezprzewodowy do ręki:

Odbiornik

- Pasmo strojenia szerokości 72MHz
- Ponad 60 kompatybilnych kanałów, w danym zakresie częstotliwości,
- 22 systemy pracujące w kanale szerokości 8MHz
- Cyfrowy system predictive diversity zapewniający pewną pracę RF
- Automatyczne skanowanie kanałów
- Synchronizacja między nadajnikiem a odbiornikiem przez port podczerwieni
- Połączenie ethernetowe.
- Szyfrowanie AES 256-bit.
- Do 60 dB, regulowane przez audio gain
- Diody wskazujące poziom peak zarówno dla audio jak I sygnału radiowego
- Odłączane anteny półfalowe
- Przełączane (mic/line) wyjście XLR
- Trwała aluminiowa konstrukcja ze szczotkowanym wykończeniem
- Uchwyty Rack w zestawie.

Nadajnik

- Pasmo przenoszenia: 20-20 kHz (±1 dB)
- Przełączana moc wyjściowa (RF) nadajnika – 1 lub 10 mW
- Możliwość wyboru opcji wyświetlania ekranu LCD. Do wyboru grupa/kanał, częstotliwość lub pozostały czas pracy
- Zasięg do 100 m
- Funkcja blokowania włącznika oraz zmiany częstotliwości
- 24-bitowa rozdzielczość oraz częstotliwość próbkowania 48 kHz ;
- 20. Mikrofon bezprzewodowy nagłowny

Nadajnik typu bodypack:

- Pasmo przenoszenia: 20-20 kHz (±1 dB)
- Przełączana moc wyjściowa (RF) nadajnika – 1 lub 10 mW
- Szyfrowanie AES 256-bit
- Możliwość wyboru opcji wyświetlania ekranu LCD. Do wyboru grupa/kanał, częstotliwość lub pozostały czas pracy
- Zasięg do 100 m
- Funkcja blokowania włącznika oraz zmiany częstotliwości
- Odłączane anteny
- Bateria do 10 godzin pracy.

Mikrofon:

- Typ przetwornika: Pojemnościowe
- Charakterystyka: kardionalna
- Pasmo przenoszenia: 45 Hz - 20 kHz
- Czułość (1 kHz): -59 dBV/Pa

Splitter wzmacniacz antenowy:

- Obsługa do 4 odbiorników
- Szerokopasmowe UHF (470-952 MHz)
- Przystosowany do montażu w szafie rack
- Anteny umieszczone na przednim panelu.

Antena pasywna szerokopasmowa:

- Charakterystyka: wszechkierunkowa
- zakres częstotliwości: 470-1100 MHz
- złącze: BNC (F)
- współpraca z systemami bezprzewodowymi
- współczynnik fali: <2:1 (50Ω)

Akumulator:

- Zakres temperatury: 0^{O}C - 45^{O}C
- Napięcie nominalne min. 3,7 V
- Pojemność nominalna min. 1320 mAh
- Prąd ładowania min 750 mAh
- Napięcie ładowania 4.2 V (±0.05 V)

Ładowarka do akumulatorów:

- Napięcie wejściowe: 15V max. 3,33 A
- Napięcie wyjściowe: 0,75 A
- Czas pełnego ładowania: max 3 h
- dioda sygnalizująca status ładowania

Wzmacniacz mocy 120W/100V:

- Wzmacniacz klasy D o szerokości pół racka z wbudowaną matrycą 2x1która pozwala miksować sygnał
- wbudowany procesor DSP współpracujący z oferowanymi kolumnami/głośnikami
- złącza GPIO
- konfiguracja wzmacniacz poprzez port USB
- 240W/70V, 120W/100V

Kolumna sufitowa wpuszczana:

- Moc maksymalna: min. 240W
- Głośnik wysokotonowy: 19mm (0,75") koksjalny
- Głośnik niskotonowy: 200mm (8")
- Pasmo przenoszenia: min. 79Hz - 21kHz
- Skuteczność: min. 93 dB
- Impedancja: 6 Ω
- Nominalny kąt pokrycia: 90° stożkowo
- Częstotliwość podzialu zwrotnicy: min. 6000 Hz
- Odczepy dla instalacji 70V: 60W, 30W, 15W, 7.5W
- System mocujący: zaciski dźwigniowe
- Budowa: maskownica: powlekana stal, wodoodporna, obudowa: stal ocynkowana,
- Połączenia: wypinane łącze, końcówki przewodów głośnikowych blokowane śrubami,

- przełącznik obrotowy, uchwyt na linkę bezpieczeństwa
- Głębokość montażu: maks. 26,5 cm
- Waga: maks. 5,5 kg.
- W zestawie: 2x szyny usztywniające do sufitu podwieszanego, osłona do malowania obudowy

Jednostka centralna:

- Procesor sterujący z przełącznikiem
- Wbudowany procesor DSP, wzmacniacz, centrum dystrybucji sygnałów HD
- Zapewnia pełną kontrolę prezentacji i routing sygnału
- Zintegrowany system sterowania, multimedialna krosownica, mikser mikrofonowy
- Wbudowana pamięć min. 256MB SDRAM i 1GB FLASH
- 2 x złącze DB9 obsługujące dwukierunkową transmisję RS0232
- 1 x złącze typu terminal block (8 pin) obsługujące 4 nadajniki podczerwieni
- 1 x złącze wejściowe typu terminal block (3 pin) dla odbiornika podczerwieni
- 1 x złącze typu terminal block (5 pin) obsługujące 4 porty typu I/O wejścia/wyjścia
- 1 x złącze typu terminal block (8 pin) obsługujące 4 izolowane przekaźniki
- 4 x złącza typu terminal block (4 pin) obsługujące magistralę systemową
- 1 x Ethernet (RJ45)
- 1 x USB do programowania jednostki
- Wejścia AV: min. 5 x HDMI, 3 x VGA, 1 x Component, 5 x Audio, 6 x Mikrofonowe, 1 x SPDIF
- Wyjścia AV: min. 2 x HDMI, 2x Audio, 2 x 20W/4-8 ohm, 1x 40W/70-100V
- Zasilanie: 230V AC
- Obudowa: wolnostojąca lub instalacyjna w standardzie rack 19”

Zasilacz systemowy 1:

- Dostarczana moc: min.90 W
- Napięcie wyjściowe 48 V DC regulowane
- Prąd wyjściowy min.1,875 A

Dotykowy panel sterujący 7”:

- 7" ekran dotykowy TFT zasilany POE
- wyposażony w pięć przycisków
- wbudowany mikrofon
- wbudowany głośnik
- obsłufga formatu H.264
- jasność min 300 cd
- wbudowany czujnik oświetlenia, SIP, wbudowana kamera

Puszka podtynkowa panela:

- Puszka podtynkowa dostosowana do dotykowego panelu sterującego zawartego w niniejszej ofercie

Panel dotykowy sterujacy bezprzewodowy:

- Pojemność: min. 32 GB
- Wyświetlacz IPS LCD

- Wyświetlacz Multi-Touch o przekątnej min. 9,7"
- Nagrywanie w jakości HD 1080p
- Rozdzielczość min. 1536 x 2048
- Sieci: Wi-Fi , Bluetooth 4.2
- Kanały: 2,4 GHz oraz 5 GHz
- Powłoka antyodblaskowa
- Funkcja Touch ID
- Bateria litowo-polimerowa o pojemności min. 30 Wh
- Wyjście mini Jack

Klawiatura sterująca (przy drzwiach):

- Klawiatura pięcio przyciskowa
- Podświetlenie LED RGB
- 2x wejście cyfrowe
- Zasilanie poprzez magistralę systemową
- Kolor czarny
- Wbudowany czujnik światła
- Wysokość 12cm, szerokość max 8 cm

Moduł sterowania oświetleniem DALI:

Dwukanałowy ściemniacz do sterowania balastami opraw świetlówkowych

- 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

Moduł sterowania silnikami:

- 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 do komunikacji z innymi urządzeniami systemu sterowania.
- 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.

- 8 programowalnych, izolowanych lokalnych wejść umożliwiających podłączenie zewnętrznych przycisków

Zasilacz systemowy 2:

- 6 portów magistrali systemowej.
- Montaż na szynie DIN
- Moc wyjściowa 60W.
- Pobór mocy 70W.
- Możliwości montażowe: montaż na szynie DIN, szerokość 6 modułów DIN.

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

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;

5.14 System rezerwacji sal oraz informacji wizualnej

Projektuje się system rezerwacji sal oraz informacji wizualnej będący rozwinięciem istniejącego w obiekcie systemu.

System rezerwacji

Przy każdej sali objętej systemem AV należy zainstalować panel 10 calowy z wbudowanym odtwarzaczem i nakładką dotykową, z pozycji którego Użytkownik może:

- Wyszukać wolną salę;
- Dokonać rezerwacji sali (dla dowolnej sali);
- Potwierdzić spotkanie;
- Wydłużyć/skrócić/usunąć spotkanie;
- Zgłosić awarię sprzętu/wyposażenia sali;
- Uzyskać widok z podziałem na miesiąc, tydzień, dzień;
- Możliwość podglądu harmonogramu zajętości dla innych sal;
- Możliwość dokonania rezerwacji dowolnej sali z dowolnego panelu;
- Wybrać język.

Powyższe czynności mogą być poprzedzone wymogiem autoryzowania się przez użytkownika definiowane z panelu administratorskiego.

Panel oferuje poniższe funkcje:

- Podświetlenie (zielone/czerwone/żółte) sygnalizujące status sali: wolna/zajęta/przed spotkaniem wraz możliwością włączenia/wyłączenia podświetlania z pozycji panelu administracyjnego.
- Jednoczesne wyświetlanie plików multimedialnych (MPEG2, MPEG4, H264, H265 wykorzystując akceleracje sprzętową, PDF, strumieni z kamer IP, obrazów JPG i PNG MP3, FLAC, OGG), www oraz tikera (płynnie przesuwający się pasek informacyjny) na ekranie odtwarzacza w dowolnie ustalonych z pozycji aplikacji zarządzającej przez administratora obszarach wyświetlania. Możliwość podziału ekranu na co najmniej 2 obszary i niezależne wyświetlanie w obszarach playlist z plikami multimedialnymi wymienionymi powyżej.
- Możliwość wyświetlania płynnie przesuwającego się paska z informacją ładowany on-line RSS lub edytowany ręcznie (60 kl/s, niezacinający się przy przejściu z jednej reklamy na inną wyświetlanej w innej części ekranu);
- Synchronizacja wyświetlanego między panelami kontentu (dla plików video) tak by w danej chwili ten same pliki multimedialne (reklamy) wyświetlały się na wszystkich panelach.
- Spełnienie wymogów bezpieczeństwa sieciowego z wykorzystaniem standardu uwierzytelniania z certyfikatem IEEE802.1x.
- Możliwość wprowadzenia/podmiany przez administratora własnego logo graficznego na widoku/interface panelu.
- Możliwość zdalnego zaplanowania włączenia/wyłączenia urządzenia (dla określonych godzin i dni w oparciu o kalendarz) przez administratora.
- Możliwość zdalnego zaplanowania wyłączenia/włączenia matrycy LCD w urządzeniu w określonych godzinach pracy (tryb nocny) przez administratora.
- Zdalne połączenie z konsolą urządzenia możliwe tylko za pomocą komputera z wgranym certyfikatem.
- Możliwość integracji z MS Exchange/Lotus/Office 365, Fidelio za pomocą panelu administracyjnego na stronie WWW.
- Możliwość komunikacji z MS Exchange poprzez serwer proxy.
- Pobieranie i wyświetlanie informacji z systemu USOS (integracja z systemem).
- Pobieranie plików multimedialnych przez jeden odtwarzacz i udostępnianie go pozostałym odtwarzaczom na zasadzie "klient od klienta".
- Przesyłanie statusów urządzeń na zasadzie “klient do klienta” i zbiorcze wysyłanie statusów urządzeń przez jeden odtwarzacz.

W głównych ciągach komunikacyjnych należy zainstalować monitory zbiorcze (min. 55”).

Należy przewidzieć panel administratorski (oprogramowanie serwerowe) oferujący następujące funkcjonalności:

- Aplikacja zarządzająca systemem działająca w oparciu o przeglądarkę www pozwalająca tworzyć playlisty z wyświetlanym contentem z uwzględnieniem czasu trwania, harmonogramów oraz contentu wyzwalanego na żądanie. Możliwość dodawania plików na playlistę z pulpitu metodą Drag&Drop (także z pozycji urządzeń mobilnych).
- Działanie w sieci IP z wykorzystaniem protokołu internetowego HTTP i HTTPS przy założeniu, że playery to klienci serwera. W przypadku braku dostępu do sieci lub fragmentu sieci wstrzymują pobieranie contentu i wznawiają w momencie uzyskania dostępu do sieci. Content HTML5 jest odtwarzany lokalnie i działa również w przypadku braku połączenia z serwerem. Możliwość pozostawiania rozkazów dla

paneli/odtwarzaczy na serwerze nawet gdy są wyłączone. W momencie uruchomienia player wykonuje listę rozkazów.

- System umożliwia raportowanie wszystkich wyświetleń contentu, obejmujące bieżący monitoring obciążenia paneli/odtwarzaczy, ich status oraz ekranu. Wszystko z poziomu strony WWW oraz wysyłanie emaili z podsumowaniem wyświetleń. Możliwość przeglądania wykresów wyświetleń (dni/godziny/panele/odtwarzacze).
- System pozwala na odtwarzanie strumieni Video z dowolnego źródła w sieci IP (H264, H265, MJPEG).
- Możliwość konfigurowania paneli/odtwarzaczy podłączonych do serwera z poziomu aplikacji zarządzającej WWW oraz dodatkowej zewnętrznej aplikacji dla systemu Windows konfigurującej playery w sieci LAN.
- Możliwość automatycznego tworzenia kopii zapasowej całej konfiguracji aplikacji zarządzającej i jej bazy danych do jednego skompresowanego pliku, tak by w przypadku awarii lub uszkodzenia przywrócić jej wszystkie ustawienia z jednego pliku.
- Wieczysta licencja na użytkowanie oprogramowania oraz dostęp do bezpłatnych aktualizacji przez okres gwarancji.
- Przypisywanie panelom/odtwarzaczom słów kluczowych oraz grupowanie techniką drag&drop działające również na smartfonach i tabletach. Możliwość wizualnego rozmieszczania paneli/odtwarzaczy na zaimportowanej mapie budynku. Przypisywanie panelom/odtwarzaczom określonych parametrów wyświetlania i ich zachowań poprzez umieszczenie danego panelu/odtwarzacza w zależności od położenia na mapie (tworzenie na mapie określonych obszarów o określonymi parametrami wyświetlania) lub na podstawie ich położenia geograficznego względem obszarów dodanych do mapy.
- Działanie całego systemu w oparciu o otwarto źródłową bazę danych na licencji BSD.
- Dostępna przez www biblioteka mediów umożliwiająca wielopoziomowe katalogowanie treści (tworzenie i edytowanie folderów) klipów.
- Szczegółowe uprawnienia użytkowników. Możliwość wizualnego nadawania i odbierania uprawnień do aplikacji zarządzającej i jej poszczególnych elementów (także możliwość nadania uprawnień do edycji pojedynczych slajdów graficznych – szablonów). Możliwość nadawania uprawnień - nadrzędnych ról kontrolujących innych użytkowników.
- Przyjmowanie komend przez panele w języku LUA z zewnętrznych systemów/urządzeń jedynie poprzez protokół HTTP.
- Umożliwienie połączenia z systemem operacyjnym panelu/odtwarzaczy tylko i wyłącznie z wykorzystaniem klucza szyfrującego (brak posiadania klucza musi uniemożliwić zdalne wejście na system odtwarzacza).
- Grupowanie urządzeń (jeden panel może być przypisany do wielu grup), wyświetlanie plików multimedialnych w oparciu o przynależność do grupy.
- Możliwość zdalnej aktualizacji/upgrade oprogramowania wyświetlającego (obejmującego powyższe funkcje).
- Możliwość odtwarzania strumieni video poprzez MULTICAST i BROADCAST, UNICAST oraz protokół HTTP.
- Możliwość dodawania strumieni IPTV do playlist oraz wyświetlanie ich w dowolnym obszarze wyświetlania.
- Panel monitoringu służący do podglądu statusów playerów/paneli - prezentacja statusu;

- Graficzna prezentacja statusu urządzeń na importowanej mapie budynku lub obszaru geograficznego.
- Bieżący monitoring obciążenia playerów wpiętych do sieci wraz ze zrzutami ekranu na żądanie.
- Status działania całego systemu generowany podstawie danych dostarczanych przez wszystkie playery/panele.
- Raportowanie wg liczby i łączny czas wyświetleń danej reklamy/klipu w podziale na eventy/godziny/dni/miesiące i nośnik. Łączny czas wyświetlania danej reklamy/klipu lub/i danego Klienta w podziale na eventy/godziny/dni/miesiące. Wyświetlenie (wartościowo, ilościowo, czasowo) z podziałem na eventy/miesiące.
- Graficzna prezentacja informacji o wyświetlaniu w formie graficznych i słupkowych wykresów.
- Możliwość eksportowania raportów do wyświetlaniu do plików PDF, CSV.

<u>System informacji wizualnej (Digital Signage)</u>

Projektuje się system informacji wizualnej, który wykorzystywał będzie wspólne monitory zbiorcze z systemem rezerwacji sal. System oferował będzie następujące funkcjonalności:

- System umożliwia wizualne centralne i zdalne zarządzanie rozdzielczościami odtwarzaczy (powierzchnia wyświetlająca), ustawienie na nim obszarów (ułożenie obszarów na ekranie przeciągając i układając je myszką) a także przypisywanie playlist do ekranów oraz dowolnej ilości obszarów (stref) na jakie zostanie podzielona powierzchnia wyświetlająca odtwarzacza.
- Możliwość określenia domyślnych właściwości dla wszystkich klipów na wybranej playliście np. wybór silnika renderującego.
- Łatwa możliwość wyświetlania aplikacji zewnętrznych producentów poprzez dodanie takiej aplikacji do playlisty by została rozesłana do playerów i tam uruchomiona na playliście lub w formie klipu uruchamianego na żądanie.
- System umożliwia oskryptowanie różnych zachowań elementów systemu w tym: przypisywanie zdarzeń do klawiszy, do myszy i ekranów dotykowych, komunikację z urządzeniami za pomocą RS-232 oraz protokołu HTTP oraz raportowanie do serwera o statusie tej komunikacji a także sterowanie natężeniem dźwięku.
- Zdalne i centralne aktualizowanie contentu przez sieć IP - ethernet, internet, wykorzystując WiFi, GSM zarówno przez WWW.
- Edytor slajdów graficznych służy do budowy edytowalnych slajdów graficznych umieszczanych jako niezależny content/klip na playliście. Edytor dostępny jest z poziomu przeglądarki WWW w ramach aplikacji zarządzającej systemem. Slajdy umożliwiają:
  - Ustawianie tła szablonu z plików:
  - video. (avi, mp4, mov, m2v, mpg, wmv),
  - zdjęcie. (jpg, png, gif),
  - jednolite tło, kolor wybierany jest z palety barw, oraz RGB,
  - Dodawanie dowolnej ilości pól tekstowych, formatowania (rozmiaru, kolor, czcionka, pochylenie, grubość, położenie).
  - Dodawanie zdjęć/video (jpg, png, gif, swf, avi, mp4, mov, m2v, mpg, flv, wmv).
  - Wyświetlanie informacji z RSS (waluty, pogoda, wiadomości) lub z dowolnego pliku xml.
  - Możliwość określenia w której sekundzie dany element szablonu ma się pojawić.
  - Przypisanie szablonów do poszczególnych klientów.

- Podgląd szablonu w czasie tworzenia edycji.
- Wybór orientacji ekranu (pionowa, pozioma).
- Przesuwanie i skalowanie elementów na szablonie za pomocą myszki.
- Upuszczanie elementów na slajd techniką drag&drop.
- Edycja treści elementów slajdu poprzez dwukrotne kliknięcie na dany element.
- Biblioteka i podgląd dostępnych szablonów wraz z ich podglądem.
- Możliwość przypisywania zdalnych URL źródeł XML/RSS dla elementów tekstowych aby wyświetlały aktualną treść w danej chwili.

- Wbudowane szablony graficzne HTML5 (gotowe szablony) wykorzystujące animacje akcelerowaną przez GPU. Między innymi:
  - Slajd (szablon) do wyświetlania komunikatów przez użytkowników wraz z możliwością wstawienia zdjęcia (w przypadku utraty ważności komunikat ma automatycznie sam wygasnąć).
  - Slajd (szablon) zawierający informacje oraz półprzezroczyste ikony pogodowe dla danej lokalizacji parametryzowane z pozycji systemu (automatycznie pobierające informacje pogodowe) oraz informacje o imieninach.
  - Slajd (szablon) z informacjami zawierającymi spis sal (pomieszczeń) wraz ze strzałkami kierunkowymi.
  - Slajd (szablon) z informacjami zawierającymi spis wydarzeń (rezerwację sal). Szablon ten z możliwością zbiorczego wyświetlania wszystkich rezerwacji sal/wydarzeń oraz w drugiej wersji z wyświetlającymi się wydarzeniami dedykowanymi dla konkretnej sali. Szablony powiązane w taki sposób by raz wpisane informacje pobierane były przez wyżej wymienione szablony.

Slajdy mają możliwość edycji treści/danych z poziomu strony WWW. Slajdy zachowują swoje dane lokalnie, a w razie braku dostępu do zdalnych danych mogą wyświetlać ostatnio pobrane informacje. Wszystkie slajdy mają możliwość informowania playera o braku danych do wyświetlenia i mają możliwość wydawania zadań odtwarzaczowi (definiowanych z poziomu aplikacji klienckiej zarządzającej np. przejść do następnego klipu itp. Ze względów bezpieczeństwa player jak i szablony mają możliwość pobierania danych uwierzytelniając się na serwerach wymagających autoryzacji HTTPS. System umożliwia wczytywanie nowych slajdów (np. własnych) z pozycji administratora. Do każdego z szablonów istnieje możliwość umieszczenia tikera (pasek z informacjami) oraz zegarka z datą w dowolnej części ekranu z pozycji aplikacji administratora. Do odtwarzania slajdów HTML5 jak i stron internetowych system używa silnika Chromium. System umożliwia wyświetlanie szablonów HTML5 wraz ze wszystkimi plikami i podkatalogami potrzebnymi do ich wyświetlenia. Aplikacja zarządzająca ma możliwość nadawania uprawnień do edycji wybranego slajdu graficznego wybranemu użytkownikowi.

System powinien zapewniać następujące funkcjonalności playerów:

- Możliwość wyświetlania zbiorczego wyświetlania rezerwacji na wielkoformatowych LCD.
- Płynne odtwarzanie plików w formatach MPEG2, MPEG4, H264, H265 wykorzystując akcelerację sprzętową oraz lokalnie ładowanych slajdów graficznych HTML5. System posiada możliwość odtwarzania na odtwarzaczach plików Power Point, PDF, strumieni z kamer IP, obrazów JPG i PNG. W przypadku odtwarzaczy wyposażonych w system Windows istnieje możliwość planowego odtwarzania plików EXE zarówno pojedynczych, jak i całych katalogów z aplikacjami. Dodatkowo system umożliwia pobieranie całych struktur katalogów z treściami HTML5 w formie generowanych automatycznie przez aplikację zarządzającą skompresowanych pojedynczych plików.

- Odtwarzanie pasków z animowanym tekstem (ticker). Możliwość określania koloru tła i czcionki i wyzwalanie paska z animowanym tekstem na żądanie (np. pojawienie się tikera dopiero po przyjściu komunikatu z zewnątrz).
- Możliwość wizualnego przypisywania skryptów w języku LUA do wszystkich zdarzeń związanych z odtwarzaniem (podczas startu odtwarzacza, podczas startu odtwarzania danego klipu).
- Przyjmowanie komend w języku LUA z zewnętrznych systemów/urządzeń jedynie poprzez protokół HTTP.
- Umożliwienie połączenie się systemem operacyjnym odtwarzaczy tylko i wyłącznie z wykorzystaniem klucza szyfrującego (brak posiadania klucza musi uniemożliwić zdalne wejście na system odtwarzacza).

Wszystkie wymienione powyżej funkcje dotyczące systemu multimedialnego powinny być realizowane w ramach jednej aplikacji.

Minimalne parametry urządzeń:

Panel rezerwacji 10" z licencją na oprogramowanie:

- 10” panel dotykowy wyposażony w system operacyjny Android
- Jasność min 350 cd/m2
- Kontrast min 350:1
- Rozdzielczość min 1280x800
- Waga max 1,5 kg i głębokość max 30mm

Monitor zbiorczy:

- Przekątna 55"-57”
- Technologia panelu: IPS
- Format: 16 : 9
- Rozdzielczość: 1,920 x 1,080 (FHD)
- Jasność: min 450 cd/m2
- Kontrast: min 1000:1
- Kąty widzenia: (H x V) 178 x 178
- Czas pracy: 24/7
- Możliwość instalacji w pionie i poziomie
- Wejścia: 3xHDMI, DP, DVI-D, Audio, USB 3.0
- Wyjścia: DP (SST), Audio
- Zewnętrzna kontrola: RS232C In/out, RJ45 In, IR Receiver In
- Rozmiar ramki: max 12 mm (T/R/L), 20 mm (B)
- Waga monitora: max 18 kg
- Wbudowane głośniki 2 x 10W
- Pamięć wewnętrzna 8GB Wbudowany moduł Wi-Fi, Czujnik temperatury, Czujnik natężenia światła, webOS 4.0, Wbudowany CMS, , Play via URL, Setting Data Cloning, Firmware Update by Network, SNMP (Ver. 1.4),

5.15 System zliczający

Na etapie realizacji należy przewidzieć system zliczający osoby. Szczegóły rozwiązań ustalić z Inwestorem na etapie realizacji (w zależności od wymagań funkcjonalnych wskazanych

przez Inwestora), gdyż w chwili obecnej na obiekcie funkcjonuje autorski system. Na potrzeby tego systemu przewidziano odpowiednią rezerwę budżetu.

Budynek	Kondygnacja	Urządzenie	nr urządzenia	nr pomieszczenia	opis pomieszczenia
A1	P02	TermowizyjnyCzujnikSufitowy	TCS-01-P02.KO.1	P02.KO.1	Komunikacja
	P02	TermowizyjnyCzujnikSufitowy	TCS-02-P02.KO.2	P02.KO.2	Komunikacja
	P02	TermowizyjnyCzujnikSufitowy	TCS-03-P02.KO.11	P02.KO.11	Komunikacja
	P02	TermowizyjnyCzujnikSufitowy	TCS-04-P02.KO.9	P02.KO.9	Komunikacja
	P02	TermowizyjnyCzujnikSufitowy	TCS-05-P02.KO.10	P02.KO.10	Komunikacja
	P01	TermowizyjnyCzujnikSufitowy	TCS-06-P01.SW.4	P01.SW.4	Komunikacja
	P01	TermowizyjnyCzujnikSufitowy	TCS-07-P01.SW.14	P01.SW.14	Komunikacja
	P01	TermowizyjnyCzujnikSufitowy	TCS-08-P01.SW.34	P01.SW.34	Przestrzeń komercyjna
	P01	TermowizyjnyCzujnikSufitowy	TCS-09-P01.SW.39	P01.SW.39	Hol wejściowy
	P01	TermowizyjnyCzujnikSufitowy	TCS-10-P01.SW.72	P01.SW.72	Przedsionek
	P01	TermowizyjnyCzujnikSufitowy	TCS-11-P01.IPP.137	P01.IPP.137	Przedsionek
	P1	TermowizyjnyCzujnikSufitowy	TCS-12-P1.CN.16	P1.CN.16	Sala seminaryjna
	P0	TermowizyjnyCzujnikSufitowy	TCS-13-P0.CJD.12	P0.CJD.12	Sala studentów
	P3	TermowizyjnyCzujnikSufitowy	TCS-14-P3.RAD.20	P3.RAD.20	Sala seminaryjna
	P4	TermowizyjnyCzujnikSufitowy	TCS-15-P4.KD.1	P4.KD.1	Sala seminaryjna
	P5	TermowizyjnyCzujnikSufitowy	TCS-16-P5.EK.17	P5.EK.17	Sala seminaryjna
	P7	TermowizyjnyCzujnikSufitowy	TCS-17-P7.UR.47	P7.UR.47	Sala seminaryjna
	P8	TermowizyjnyCzujnikSufitowy	TCS-18-P8.MP.7	P8.MP.7	Pok. seminaryjny
	P10	TermowizyjnyCzujnikSufitowy	TCS-19-P10.CO.13	P10.CO.13	Sala seminaryjna
	P10	TermowizyjnyCzujnikSufitowy	TCS-20-P10.CO.100	P10.CO.100	Sala seminaryjna
	P10	TermowizyjnyCzujnikSufitowy	TCS-21-P10.CO.90	P10.CO.90	Sala seminaryjna
	P11	TermowizyjnyCzujnikSufitowy	TCS-22-P11.GE.12	P11.GE.12	Sala seminaryjna
	P11	TermowizyjnyCzujnikSufitowy	TCS-22-P11.NR.32	P11.NR.32	Sala seminaryjna
	P11	TermowizyjnyCzujnikSufitowy	TCS-23-P11.NR.33	P11.NR.33	Sala seminaryjna
	P12	TermowizyjnyCzujnikSufitowy	TCS-24-P12.SM.33	P12.SM.33	Sala seminar. - debryfingowa
	P12	TermowizyjnyCzujnikSufitowy	TCS-25-P12.SM.17	P12.SM.17	Sala seminar. - debryfingowa
	P14	TermowizyjnyCzujnikSufitowy	TCS-27-P14.PiO.58	P14.PiO.58	Sala seminaryjna
	P14	TermowizyjnyCzujnikSufitowy	TCS-26-P14.PiO.58	P14.PiO.58	Sala seminaryjna
	P14	TermowizyjnyCzujnikSufitowy	TCS-28-P14.PH.31	P14.PH.31	Sala seminaryjna
	P15	TermowizyjnyCzujnikSufitowy	TCS-31-P15.CH.55	P15.CH.55	Sala seminaryjna
	P15	TermowizyjnyCzujnikSufitowy	TCS-30-P15.CH.54	P15.CH.54	Sala seminaryjna
	P15	TermowizyjnyCzujnikSufitowy	TCS-32-P15.ENK.1	P15.ENK.1	Sala seminaryjna
	P16	TermowizyjnyCzujnikSufitowy	TCS-33-P16.PO.2	P16.PO.2	Sala seminaryjna
	P16	TermowizyjnyCzujnikSufitowy	TCS-34-P16.NN.12	P16.NN.12	Sala seminaryjna
A2	P02	TermowizyjnyCzujnikSufitowy	TCS-01-P02-KO.5-1	P02.KO.5-1	Komunikacja-1
	P02	TermowizyjnyCzujnikSufitowy	TCS-02-P02.KO.14	P02.KO.14	Korytarz
	P02	TermowizyjnyCzujnikSufitowy	TCS-03-P02.LD.13	P02.LD.13	Sala ćwiczeniowa
	P01	TermowizyjnyCzujnikSufitowy	TCS-04-P01.POZ.28	P01.POZ.28	Wiatrołap
	P01	TermowizyjnyCzujnikSufitowy	TCS-05-P01.POZ.30	P01.POZ.30	Wiatrołap
	P01	TermowizyjnyCzujnikSufitowy	TCS-06-PO1.POZ.29	P01.POZ.29	Wiatrołap
	P01	TermowizyjnyCzujnikSufitowy	TCS-07-P01.KO.9	P01.KO.9	Komunikacja
	P01	TermowizyjnyCzujnikSufitowy	TCS-08-P01.END.2	P01.END.2	Komunikacja
	P01	TermowizyjnyCzujnikSufitowy	TCS-09-P01.KO.7	P01.KO.7	Komunikacja
	P01	TermowizyjnyCzujnikSufitowy	TCS-10-P01.KO.5	P01.KO.5	Komunikacja
	P01	TermowizyjnyCzujnikSufitowy	TCS-11-P01.TK.27	P01.TK.1	Przedsionek
	P0	TermowizyjnyCzujnikSufitowy	TCS-12-P00.POR.1	P00.IP.112-3	Pom. teletechniczne-3
	P0	TermowizyjnyCzujnikSufitowy	TCS-13-P00.IP.109	P00.IP.111	Hol
	P0	TermowizyjnyCzujnikSufitowy	TCS-14-P00.ADM.1	P00.ADM.1	Sala seminaryjna
	P0	TermowizyjnyCzujnikSufitowy	TCS-15-P00.ADM.1	P00.ADM.1	Sala seminaryjna
	P0	TermowizyjnyCzujnikSufitowy	TCS-16-P00.COK.1	P00.COK.1	Sala seminaryjna
	P1	TermowizyjnyCzujnikSufitowy	TCS-18-P1.AP.5	P1.AP.5	Pom. szkoleniowe

Na szaro zaznaczono obszary wyłączone z zakresu niniejszego opracowania.

Projektowany system dla każdego przejścia składać się będzie z czujnika termowizyjnego, zasilacza i modułu zliczającego podłączonego do sieci LAN. System należy wyposażyć w

oprogramowanie umożliwiające zdalny odczyt i archiwizację danych z systemu z wykorzystaniem sieci strukturalnej LAN dzięki czemu będzie to możliwe na dowolnym komputerze (należy założyć instalacje oprogramowania na minimum 3 komputerach wskazanych przez dział Informatyczny Inwestora). Podczas realizacji należy ścisłe współpracować z działem informatycznym Inwestora z uwagi na trwające testy prototypowego systemu w istniejącej części szpitala.

Czujnik termowizyjny (dopuszcza się również kamerę termowizyjną) należy zamontować na suficie (lub na ścianie na wsporniku), bezpośrednio za drzwiami do danego pomieszczenia lub w korytarzu. Czujnik / kamera powinna być zainstalowana na wysokości od około 2.2m do 3m i umożliwiać objecie monitoringiem przejście o szerokości do około 2.5m. Z uwagi na publiczny charakter przetargu nie wskazuje się konkretnego producenta sprzętu w związku z powyższym wysokość montażu należy dostosować do wytycznych ostatecznie wybranego producenta sprzętu. Podczas montażu należy zwrócić szczególną uwagę na wejścia do budynku ze strefy zewnętrznej, tak aby czynniki zewnętrzne nie zakłócały pracy czujnika.

Rozmieszczenie czujników pokazano na rzutach instalacji sieci strukturalnej LAN.

Projektuje się zastosowanie termowizyjnych czujników dedykowanych do systemów liczenia osób. Projektowana technologia pozwalać będzie na dopasowywanie się czujnika do temperatury otoczenia i wykrywanie obiektów o temperaturze wykraczającej poza otoczenie. Detektor pracować będzie kierunkowo tzn. będzie odróżniać osoby wchodzące od wychodzących i generować inne impulsy w obu przypadkach. Wbudowany mikroprocesor zapewniać będzie wysoką odporność na zakłócenia, dostosowywanie się do zmiennych warunków pracy oraz pełną analizę obrazu termicznego. Detektor posiadać będzie wyjście przekaźnikowe NC zapewniające możliwość podłączenia do dowolnego urządzenia zewnętrznego.

Do kamery należy doprowadzić okablowanie sygnałowe oraz zasilające (typ okablowania wskazano na schemacie blokowym) z wykorzystaniem projektowanych tras kablowych dedykowanych na potrzeby instalacji teletechnicznych. Zakłada się wykorzystanie kamer i modułów zasilanych napięciem 12V DC.

Moduł zliczający wraz z zasilaczem należy zamontować w najbliższym pomieszczeniu technicznym na szynie DIN w projektowanej szafie RACK (dopuszczalny jest montaż w rozdzielnicy elektrycznej).

5.16 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.

Wzdłuż głównych ciągów komunikacyjnych przewiduje się układanie przewodów w korytkach metalowych nad sufitem podwieszanym lub w korytkach kablowych w podłodze technicznej. Przy odejściach od głównych tras kablowych do poszczególnych pomieszczeń okablowanie należy układać w rurkach elektroinstalacyjnych natynkowo (nad sufitem podwieszanym) lub w korytkach kablowych o szerokości 50mm (nad sufitem podwieszanym) lub podtynkowo (na odejściach od przestrzeni nad sufitem podwieszanym do gniazd lub urządzeń końcowych). Dopuszcza się rozprowadzenie okablowania (na odejściach od głównych tras kablowych) łącznie z obsługą korytek kablowych w rurkach elektroinstalacyjnych układanych pod tynkiem.

Z uwagi na ograniczoną przestrzeń nad sufitem podwieszanym dopuszcza się rozprowadzenie okablowania do poszczególnych pomieszczeń lub grup pomieszczeń przez pomieszczenia sąsiadujące (dotyczy zespołów kablowych w rurkach elektroinstalacyjnych, koryt 50mm i pojedynczych kabli).

Dla projektowanych instalacji należy stosować okablowanie w izolacji i powłoce w klasie reakcji na ogień B2ca-s1b,d1,a1 w obrębie dróg ewakuacyjnych oraz klasie Dca-s2,d1,a2 w pozostałych przestrzeniach - zgodnie z rozporządzeniem CPR oraz normą N SEP-E-007:2017-09. Na zewnątrz budynków (np. instalacje techniczne na dachu), poza drogami ewakuacyjnymi dopuszcza się stosowanie zespołów kablowych w klasie Eca.

Na potrzeby systemów pożarowych należy zainstalować zespoły kablowe o cechach E90. Zespoły kablowe należy mocować do podłoża betonowego, kamienia lub innego posiadającego odpowiednią do zespołu kablowego klasę odporności ogniowej.

Odstępy mocowań uchwytów zespołów kablowych należy stosować zgonie z dokumentacją producenta systemu i odpowiednią Aprobata Techniczną

6 UWAGI

- 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. z 2015 r., poz. 1422, 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.
- Brak wyszczególnienia jakiegokolwiek elementu, który może być zawarty w dokumentacji warsztatowej lub jest wymagany względami technologicznymi, aby skończone instalacje lub budynek uznać za kompletny i zgodny z założeniami projektowymi, nie zwalnia Wykonawcy z obowiązku wykonania tych elementów i nie stanowi podstawy do roszczenia zakresu prac pomiędzy Inwestorem a Wykonawcą.
- W zakresie Wykonawcy jest bieżąca koordynacja prac na budowie. Brak wyszczególnienia jakiegokolwiek elementu lub brak jego inwentaryzacji, który może mieć wpływ na realizację nie stanowi podstawy do roszczenia zakresu prac pomiędzy Inwestorem a Wykonawcą.
- Wykonawca musi przewidzieć modernizację istniejących instalacji, także tych niebędących w zakresie niniejszej dokumentacji, jeśli będzie to wymagane względami technologicznymi (uwzględniając również pomieszczenia poza zakresem opracowania).
- Z uwagi na publiczny charakter realizacji inwestycji wszelkie obliczenia i dobory takich elementów jak pojemności akumulatorów, pojemności dysków itp. Generalny Wykonawca zobowiązany jest wykonać na etapie realizacji w oparciu o dane Producentów poszczególnych systemów zaakceptowanych przez Inwestora i Nadzór Autorski.
- W przypadku wybranych pomieszczeń (w szczególności: Hemodynamika, Endoskopia i chirurgia jednego dnia, Intensywna terapia, Mikrobiologia, Blok operacyjny, Centralna sterylizacja, Izba przyjęć) urządzenia tam stosowane powinny posiadać cechy bakteriobójcze (powłoki antybakteryjne) oraz powinny posiadać wydawany przez PZH Atest Higieniczny dopuszczający zastosowania urządzeń „dla obiektów służby zdrowia" oraz „dla bloków operacyjnych i innych obiektów o podwyższonych wymaganiach higienicznych"
- Wyprowadzenia na dach okablowania należy odpowiednio zabezpieczyć przed wpływem warunków atmosferycznych (przeciwwilgociowo, promienie UV itp.)
- Prace powinny być wykonane przez przeszkolonych instalatorów.
- Przy układaniu kabli, przewodów, zachować normatywne odległości pomiędzy kablami lub przewodami silnoprądowymi od przewodów niskoprądowych.
- Przejścia przez przegrody budowlane należy uszczelnić zgodnie z klasą odporności pożarowej EI przegrody.
- Metalowe części szaf i skrzynek połączyć z systemem połączeń wyrównawczych.

- 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.

7 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.

Akceptacje urządzeń i materiałów do rozwiązań projektowych są możliwe po uzyskaniu jednoznacznej akceptacji Zamawiającego, jedynie w przypadku rozwiązań co najmniej równorzędnych konstrukcyjnie, funkcjonalnie i technicznie. Propozycji takiej winna towarzyszyć kompletna informacja: rysunki, obliczenia, specyfikacje, proponowana technologia budowy oraz tabela porównawcza parametrów – są to niezbędne informacje do oceny przez nadzór nad budową.

8 ZAŁĄCZNIKI

[1] Przykładowe obliczenia doboru akumulatorów Systemu Sygnalizacji Pożarowej
[2] Przykładowe obliczenia obciążalności pętli Systemu Sygnalizacji Pożarowej