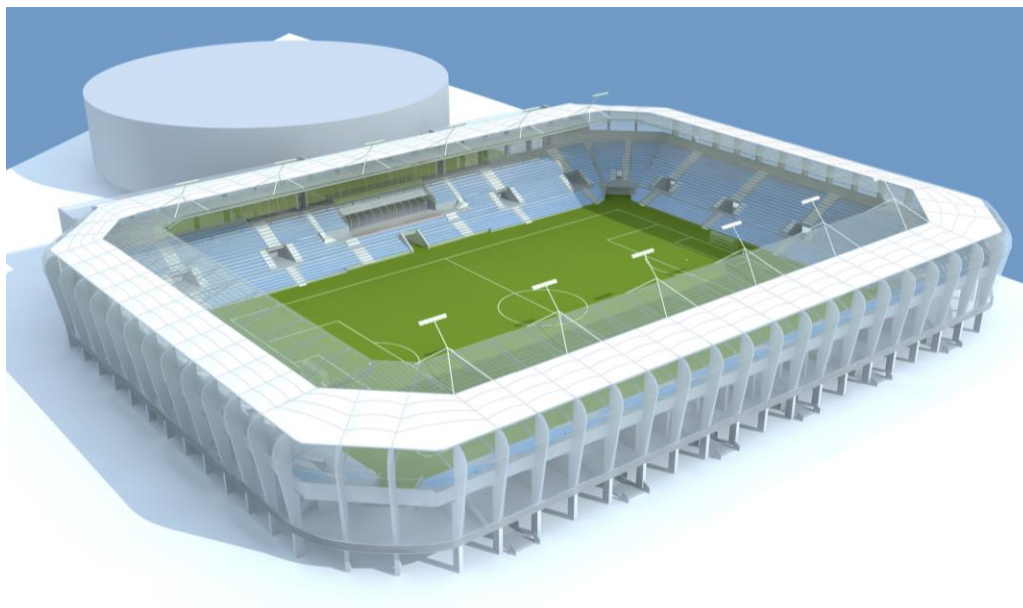


EGZ. pdf

PROJEKT WYKONAWCZY **BUDOWA STADIONU PIŁKARSKIEGO** **(NA TERENIE ISTNIEJĄCEGO STADIONU)** **PRZY ULICY STRUGA W RADOMIU**

część działki nr ewid. 78 przy ul. Andrzeja Struga / 11 Listopada
i część działki nr ewid. 81 przy ul. Stanisława Zbrowskiego



Inwestor: **MIEJSKI OŚRODEK SPORTU I REKREACJI
W RADOMIU Sp. z o.o.**
ul. Gabriela Narutowicza 9
26-600 Radom

Projektant: **ROSA-BUD S.A.**
26-600 Radom, ul. Gazowa 5/7

WOJCIECH GĘSIĄK STUDIO ARCHITEKTONICZNE
26-600 Radom, ul. Chrobrego 22

Branża: **INSTALACJE ELEKTRYCZNE NISKOPRĄDOWE**

Tom: **V b**

Projektant: mgr inż. Grzegorz Mazur
Nr upr. MAP/0049/PWOE/11

Sprawdzający: mgr inż. Krzysztof Filipak
Nr upr. MAP/0131/PWOE/06

Radom luty 2017 r.

Spis zawartości dokumentacji:

CZĘŚĆ I: OPIS

1.	Przedmiot opracowania.....	6
2.	Zakres opracowania	6
3.	Założenia projektowe.....	6
4.	Dane techniczne obiektu charakteryzujące wpływ na środowisko.....	8
4.1.	Oddziaływanie i emisja szkodliwych czynników	8
4.2.	Wpływ obiektu na drzewostan i glebę	8
5.	Rozwiązania zasadniczych elementów wyposażenia budowlano – instalacyjnego .	8
5.1.	Stan istniejący	8
5.2.	Lokalizacja głównych urządzeń	8
5.3.	Koncepcja prowadzenia instalacji dla projektowanych systemów	8
6.	Opis funkcjonalny systemu telewizji dozorowej	9
6.1.	Rozwiązanie techniczne	10
6.2.	Instalacja systemu monitoringu wizyjnego	10
6.3.	Wymagania dla systemu transmisji	10
6.4.	Instalacja zasilania urządzeń systemu CCTV	10
6.5.	Oprogramowanie zarządzające sygnałem wizyjnym	10
7.	Instalacja nagłośnienia	12
7.1.	Specyfikacja ogólna systemu	12
7.2.	Specyfikacja szczegółowa urządzeń głośnikowych	13
7.3.	Okablowanie	16
7.3.1.	Okablowanie głośnikowe.....	16
7.3.2.	Okablowanie sygnałowe	16
8.	Instalacje teleinformatyczne (okablowanie strukturalne)	16
8.1.	Wymagania podstawowe:.....	16
8.2.	Specyfikacja techniczna urządzeń instalacji okablowania strukturalnego.....	18
8.2.1.	Przewód światłowodowy	18
8.2.2.	Przewód typu skrętka.....	18
8.2.3.	Punkt logiczny (PL)	19
8.2.4.	Adapter kątowy 2xRJ45 (45x45).....	20
8.2.5.	Ekranowany moduł RJ45 kategorii 6A.....	20
8.2.6.	Modułarny panel krosowy 24xRJ45 1U	21
8.2.7.	Przełącznica światłowodowa	21
8.2.8.	Szafy dystrybucyjne.....	21
8.3.	Administracja i dokumentacja.....	22
8.4.	Odbiór i pomiary sieci.....	22

8.5.	Wymagania dla instalatora	23
8.6.	Wymagania gwarancyjne	23
8.7.	Uwagi końcowe.....	25
9.	System sprzedaży i kontroli biletów z identyfikacją kibiców	25
9.1.	Przedmiot i zakres opracowania.....	25
9.2.	Podstawa opracowania	26
9.3.	Wytyczne realizacyjne	26
9.4.	Definicje	27
9.5.	Licencjonowanie	29
9.6.	Opis ogólny systemu	29
9.7.	Wymagania systemowe i platforma serwerowa	31
9.7.1.	Platforma serwerowa	31
9.7.2.	Serwery funkcjonalne Systemu	32
9.7.3.	Monitoring poprawnej pracy Systemu.....	33
9.7.4.	Firewall - Zabezpieczenie serwera WWW	34
9.7.5.	Backup Systemu	34
9.7.6.	Pozostałe wymagania systemowe	35
9.8.	Moduł Budowania i Zarządzania Bazą Klientów	36
9.8.1.	Typy Klientów	36
9.8.2.	Zarządzanie bazą klientów.....	37
9.8.3.	Karty Klienta/Kibica.....	38
9.8.4.	Aplikacja Rejestracji Mediów i Wydawania Akredytacji	39
9.8.5.	Wydawanie identyfikatorów wewnętrznych.....	41
9.9.	Moduł Sprzedaży Dokumentów Wejściowych	42
9.9.1.	Ogólne wymagania i ustawienia konfiguracyjne Modułu	42
9.9.2.	Rodzaje i typy Dokumentów Wejściowych	43
9.9.3.	Szczegółowe funkcjonalności Modułu	45
9.9.4.	Kanały dystrybucji	46
9.9.5.	Wyposażenie i funkcjonalność Punktów Sprzedaży	46
9.9.6.	Raporty i statystyki Modułu	47
9.10.	Moduł Kontroli Biletów i Identyfikacji Kibiców	48
9.10.1.	Budowa Modułu Kontroli Biletów i Identyfikacji Kibiców	48
9.10.2.	Funkcjonalność Modułu Kontroli Biletów i Identyfikacji kibiców	48
9.10.3.	Sprawdzarki biletowe do bramek obrotowych.....	49
9.10.4.	Sygnalizatory świetlne dla ochrony	50
9.11.	Organizacja logistyczna imprez i obiektu	50
9.11.1.	Organizacja wejścia na obiekt.....	50

9.11.2.	Identyfikacja kibiców	50
9.11.3.	Obsługa specjalnych grup kibiców	51
9.11.4.	Rozpatrywanie reklamacji.....	52
9.12.	Integracja Modułu Kontroli Biletów i Identyfikacji Kibiców z Systemem CCTV 52	
9.13.	Okablowanie elektryczne i sygnałowe	53
10.	System sygnalizacji włamania i napadu	53
10.1.	Charakterystyka zastosowanych urządzeń	53
10.2.	Charakterystyka ogólna systemu	54
11.	System kontroli dostępu.....	54
11.1.	System kontroli dostępu - wymagania	54
11.2.	Hardware systemu	55
11.3.	Software.....	55
11.4.	Urządzenia wchodzące w skład SKD.....	57
12.	System integracji.....	59
12.1.	Warstwa sprzętowa	60
13.	System videodomofonowy i interkomowy	60
14.	Instalacja RTV	60
15.	System sygnalizacji pożaru.....	60
15.1.1.	Organizacja alarmowania systemu	63
15.1.2.	Automatyczne powiadamianie PSP	64
15.1.3.	Konfiguracja systemu i dobór urządzeń	65
15.1.4.	Ogólny opis	65
15.1.5.	Moduły funkcjonalne centrali	65
15.1.6.	Kontroler centrali sygnalizacji pożarowej	66
15.1.7.	Redundancja centrali sygnalizacji pożarowej	69
15.1.8.	Zasilacz.....	69
15.1.9.	Moduł liniowy	69
15.1.10.	Automatyczne detektory pożaru – czujki punktowe	70
15.1.11.	Ręczny ostrzegacz pożaru	73
15.1.12.	Wskaźnik zadziałania	74
15.1.13.	Moduł sterujący 8 wejść, 1 wyjście – typ 1	74
15.1.14.	Moduł sterujący 8 wyjść – typ 2.....	75
15.1.15.	Okablowanie dla systemu ppoż.....	76
15.1.16.	Zasilanie podstawowe i awaryjne	77
15.1.17.	Współpraca z innymi systemami	78
15.1.18.	Wytyczne w zakresie przeglądów i konserwacji.....	78

16.	System BMS	78
16.1.	Komponenty systemu BMS.....	79
16.2.	Centralne stanowisko nadzoru.....	79
16.3.	Sterowniki BMS	80
16.4.	Rozdzielnice BMS.....	81
16.5.	Funkcjonalność systemu BMS	81
16.6.	Kontrola układów SZR.....	81
16.7.	Kontrola zasobów energetycznych budynku	82
16.8.	Monitoring zużycia energii elektrycznej	82
16.9.	Sterowanie oświetleniem.....	82
16.10.	Monitoring UPS.....	82
16.11.	Monitoring rozdzielnic elektrycznych.....	82
17.	Dane techniczne obiektu charakteryzujące wpływ na środowisko.....	83
17.1.	Oddziaływanie i emisja szkodliwych czynników.....	83
17.2.	Wpływ obiektu na drzewostan i glebę.....	83
18.	Warunki ochrony przeciwpożarowej	83
19.	Uwagi końcowe	83

CZĘŚĆ II: GRAFICZNA

I.p.	nr rys	nazwa
1	PW-S-TT-R-IB,II-01	Rozmieszczenie elementów instalacji SAP - Rzut poziomu "0"
2	PW-S-TT-R-IB,II-02	Rozmieszczenie elementów instalacji SAP - Rzut poziomu "1"
3	PW-S-TT-R-IB,II-03	Rozmieszczenie elementów instalacji SAP - Rzut poziomu "2"
4	PW-S-TT-R-IB,II-04	Rozmieszczenie elementów instalacji teletechnicznych - Rzut poziomu "0"
5	PW-S-TT-R-IB,II-05	Rozmieszczenie elementów instalacji teletechnicznych - Rzut poziomu "1"
6	PW-S-TT-R-IB,II-06	Rozmieszczenie elementów instalacji teletechnicznych - Rzut poziomu "2"
7	PW-S-TT-S-IB,II-07	Schemat blokowy instalacji BMS dla stadionu
8	PW-S-TT-S-IB,II-08	Schemat blokowy instalacji nagłośnienia stadionu

1. Przedmiot opracowania

Przedmiotem opracowania jest projekt wykonawczy instalacji elektrycznych niskoprądowych dla zadania pn.: Przebudowa stadionu piłkarskiego przy ul. Struga w Radomiu. Realizacja instalacji następować będzie w dwóch etapach:

- Etap I b,
- Etap II.

Zakres każdego z etapów zawarty jest w części Architektonicznej.

2. Zakres opracowania

Niniejsze opracowanie obejmuje:

- System telewizji dozorowej CCTV,
- Instalacja nagłośnienia,
- Instalacje teleinformatyczne (okablowanie strukturalne),
- System sprzedaży i kontroli biletów z identyfikacją kibiców,
- System sygnalizacji włamania i napadu oraz kontroli dostępu,
- System videodomofonowy i interkomowy,
- Instalacja RTV,
- System sygnalizacji pożaru,
- System BMS.

3. Założenia projektowe

Założenia do niniejszego opracowania stanowią:

- Program funkcjonalno - użytkowy,
- uzgodnienia międzybranżowe,
- Zlecenie Inwestora,
- Rzuty architektoniczne obiektu,
- Ustawa Prawo Budowlane,
- Rozporządzenie MSWiA z dnia 10 stycznia 2011r. w sprawie sposobu utrwalania przebiegu imprezy masowej,
- Ustawa z dnia 20 marca 2009r. o bezpieczeństwie imprez masowych wraz z nowelizacją z dnia 10 czerwca 2010 r.,
- Ustawa z dnia 31 sierpnia 2011r.o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw,
- Rozporządzenie MSWiA z dnia 27 kwietnia 2010 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. Nr 143, poz. 1002) ze zmianami z dnia 27 kwietnia 2010 roku.(Dz. U. Nr 85 poz. 553),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010r. w sprawie ochrony przeciwpożarowej budynków, innych

- obiektów budowlanych i terenów,
- Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 w sprawie warunków technicznych jakim powinny odpowiadać budynki i ich usytuowanie (zmiany z dn. 12 marca 2009r. Dz.U. nr 56) z późniejszymi zmianami,
 - Ustawa z dnia 24 sierpnia 1991r. o ochronie przeciwpożarowej, (Dz. U. z 2002r Nr 147, poz. 1229 z późniejszymi zmianami),
 - Specyfikacja techniczna PKN-CEN/TS 54-14. Systemy sygnalizacji pożarowej. Część 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacja”,
 - Zbiór wytycznych i materiałów do projektowania systemów sygnalizacji pożarowej - mgr inż., Jerzy Ciszewski ITB,
 - „Zasady sterowania automatycznymi urządzeniami przeciwpożarowymi przez systemy sygnalizacji przeciwpożarowej” – mgr inż. Janusz Sawicki, ITB,
 - ISO/IEC11801:2002/Am2:2010 - Information technology - Generic cabling for customer premises,
 - PN-EN 50173-1:2011 Technika Informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne,
 - PN-EN 50173-2:2008/A1:2011 Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Budynki biurowe,
 - PN-EN 50174-1:2010/A1:2011 Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja i zapewnienie jakości,
 - PN-EN 50174-2:2010/A1:2011 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-ISO/IEC 14763-3:2009/A1:2010 Technika informatyczna - Implementacja i obsługa okablowania w zabudowaniach użytkowych - Część 3: Testowanie okablowania światłowodowego,
 - PN-EN 50310:2007 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym.
 - Norma PN-EN 50131-1-2009 Systemy alarmowe, Systemy sygnalizacji włamania i napadu, Część 1: Wymagania systemowe.
 - Specyfikacja Techniczna PKN-CLC/TS 50131-7-2011 Systemy alarmowe, Systemy sygnalizacji włamania i napadu, Część 7: Wytyczne stosowania
 - PN-EN 50132-7:2003 Systemy alarmowe - Systemy dozorowe CCTV

stosowane w zabezpieczeniach - Część 7: Wytyczne stosowania,

- PN-EN 50133-1:2007 Systemy alarmowe -- Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia -- Część 1: Wymagania systemowe.
- Instrukcje, dokumentacje techniczno-ruchowe i wytyczne dostawcy urządzeń,
- Obowiązujące normy i przepisy.

4. Dane techniczne obiektu charakteryzujące wpływ na środowisko

4.1. Oddziaływanie i emisja szkodliwych czynników

Projektowane instalacje nie wpływają negatywnie na środowisko. Występowania wyższych harmonicznych od dopuszczalnych nie przewiduje się. Występowania pól elektromagnetycznych, wibracji i drgań pochodzenia energetycznego nie przewiduje się.

4.2. Wpływ obiektu na drzewostan i glebę

Projektowana instalacja nie wpływa na stan drzewostanu i wody powierzchniowe i podziemne.

5. Rozwiązania zasadniczych elementów wyposażenia budowlano – instalacyjnego

5.1. Stan istniejący

W związku z budową nowego obiektu nie występuje stan istniejący instalacji teletechnicznych. Wszystkie systemy zostaną zaprojektowane od podstaw.

5.2. Lokalizacja głównych urządzeń

W pomieszczeniach technicznych na terenie stadionu zlokalizowane zostaną urządzenia systemów teletechnicznych (zasilacze, kontrolery systemowe, urządzenia teletransmisyjne), wzmacniacze systemu nagłośnieniowego zlokalizowane zostaną w szafach rack 19” w pomieszczeniach:

- Serwerownia pom. nr [0]-S-Z-01,
- Pom. techniczne nr [0]-S-Z-14.

Pozostałe pomieszczenia z lokalizacją urządzeń teletechnicznych zostały pokazane w części graficznej.

Instalacje teletechniczne są wspólne dla obszaru hali i stadionu. M.in. główne serwery systemu BMS, CCTV, Integracji Budynkowej, Biletowego znajdować się będą w serwerowni w hali. Oba obiekty (hala, stadion) zostały połączone siecią LAN.

5.3. Koncepcja prowadzenia instalacji dla projektowanych systemów

Wszystkie kable i przewody będą prowadzone i ułożone w następujący sposób:

- W pomieszczeniach technicznych, rurki / listwy PCV – przewody bez odporności ogniowej.
- W przestrzeni międzysufitowej: trasa metalowa w ciągach komunikacyjnych - przewody bez odporności ogniowej, rurki / listwy PCV w

pozostałych pomieszczeniach – przewody bez odporności ogniowej. Przewody pętli adresowalnych systemu SAP – rurki / listwy PCV prowadzone z zachowaniem zasady dwóch różnych tras do transmisji danych.

- W przestrzeni międzysufitowej: na certyfikowanych uchwytach. Poza przestrzenią sufitową (m.in. podejścia widoczne) podtynkowo na certyfikowanych uchwytach (w pom. technicznych, piwnicy nadtynkowo). Dotyczy zespołów kablowych o odporności ogniowej.

- W kanalizacji teletechnicznej: układać odpowiedni światłowód do stosowania w kanalizacji pierwotnej.

6. Opis funkcjonalny systemu telewizji dozorowej

Zadaniem systemu CCTV jest podniesienie poziomu bezpieczeństwa na obiekcie, wspomaganie służb ochrony oraz porządkowych, dostarczenie materiału dowodowego w ewentualnych procesach sądowych. System telewizji dozorowej zaprojektowano na całym obiekcie i wokół niego.

Koncepcja budowy systemów telewizji dozorowej na obiektach, gdzie będą odbywać się imprezy masowe, podlega w Polsce następującym wytycznym (Rozporządzenia MSWiA z dnia 10 stycznia 2011 r. w sprawie sposobu utrwalania przebiegu imprezy masowej):

§ 4. 1. Miejscami podlegającymi obowiązkowej rejestracji obrazu są:

- 1) kasy biletowe na terenie imprezy masowej – w przypadku imprezy odpłatnej;
- 2) bramy, furtki i inne miejsca przeznaczone do wejścia uczestników na teren imprezy masowej;
- 3) drogi dla służb ratowniczych, drogi ewakuacyjne oraz ciągi komunikacyjne na terenie imprezy masowej z wyłączeniem klatek schodowych;
- 4) parkingi zorganizowane na terenie imprezy masowej;
- 5) sektory dla uczestników imprezy masowej;
- 6) płyta boiska lub scena.

2. Miejsca, o których mowa w ust. 1 pkt 1 – 4, znajdują się w polu widzenia co najmniej jednego urządzenia rejestrującego obraz, a miejsca, o których mowa w ust. 1 pkt 5 i 6, znajdują się w polu widzenia co najmniej dwóch urządzeń rejestrujących obraz.

3. Urządzenia rejestrujące obraz umieszcza się w sposób umożliwiający:

- 1) rejestrację obrazu I, II i IV kategorii w miejscach, o których mowa w ust. 1 pkt 5 i 6;
- 2) rejestrację obrazu III kategorii w miejscach, o których mowa w ust. 1 pkt 1, 2, 3 i 4.

4. Miejscami podlegającymi obowiązkowej rejestracji dźwięku są sektory dla uczestników imprezy masowej oraz płyta boiska lub scena.

W związku z powyższym wymienione powyżej miejsca bezwzględnie objęto systemem kamer.

W rozporządzeniu zdefiniowano następujące minimalne parametry obrazu oraz dźwięku:

§ 9. Parametry zarejestrowanego podczas imprezy masowej obrazu dla przedmiotu o wysokości 50 cm wynoszą odpowiednio:

- 1) przy rejestracji obrazu I kategorii - wysokość co najmniej 500 pikseli;

- 2) przy rejestracji obrazu II kategorii - wysokość co najmniej 250 pikseli;
- 3) przy rejestracji obrazu III kategorii - wysokość co najmniej 50 pikseli;
- 4) przy rejestracji obrazu IV kategorii - wysokość co najmniej 12 pikseli.

§ 10. Urządzenia rejestrujące dźwięk podczas imprezy masowej powinny umożliwić zrozumienie treści nagranych haseł i okrzyków oraz określić sposób zachowywania się uczestników imprezy masowej. Parametry tych urządzeń powinny zapewniać rejestrację sygnału akustycznego w paśmie częstotliwości od 300 Hz do 4000 Hz, przy minimalnej dynamice 50 dB.

6.1. Rozwiązanie techniczne

System CCTV składa się z:

- kamer i mikrofonów;
- niezbędnej infrastruktury zasilająco-sterowniczej;
- urządzeń rejestrujących dźwięk i video;
- urządzeń wyświetlających i sterujących pracą systemu;

W głównym punkcie dystrybucyjnym (GPD) zostaną zlokalizowane główne urządzenia serwerowe, rejestrujące. W pośrednich punktach dystrybucyjnych (PPD) zbiegać się będą linie zasilająco – sterujące.

6.2. Instalacja systemu monitoringu wizyjnego

System CCTV zaprojektowany, aby spełnić wymagania rozporządzenia MSWiA z dnia 10 stycznia 2011r. wskazującego miejsca podlegające obowiązkowej rejestracji. Aby spełnić wymagania ww. rozporządzenia, odnoszącego się do czterech kategorii zarejestrowanego podczas imprezy masowej obrazu, system CCTV oparto o rozwiązania w technologii IP. Kamery są urządzeniami typu dzień/noc z filtrem podczerwieni.

Do transmisji obrazu w sieci IP użyto przewodu typu skrętka oraz światłowodu. Linie transmisyjne od punktów kamerowych zostaną zabezpieczone przeciwprzebieciowo.

6.3. Wymagania dla systemu transmisji

Pomiędzy punktami dystrybucyjnymi, a GPD transmisja odbywa się za pomocą medium światłowodowego.

6.4. Instalacja zasilania urządzeń systemu CCTV

Kamery stałopozycyjne zasilane są zgodnie z PoE IEEE 802.3af.

Wszystkie urządzenia systemu monitoringu podłączone zostaną po zasilaczu awaryjnym UPS, oraz będą rezerwowane zasilaniem z agregatu prądotwórczego.

6.5. Oprogramowanie zarządzające sygnałem wizyjnym

System zarządzania sygnałem wizyjnym (VMS) służy do obsługi cyfrowego sygnału wizyjnego i fonicznego oraz danych w dowolnej sieci IP. Umożliwia zarządzanie

zdarzeniami i alarmami, monitorowanie stanu systemu, a także administrowanie operatorami i priorytetami. Elastyczny program licencji na oprogramowanie umożliwia swobodne dodawanie kamer, stacji roboczych i opcji w miarę wzrostu wymagań.

Oprogramowanie umożliwia dokonywanie podglądu na żywo oraz odtwarzanie zapisanych obrazów z dowolnego miejsca, w dowolnym czasie i z dowolnej lokalizacji. Kamery, rejestratory czy centra monitoringu mogą być umieszczone w wybranym miejscu sieci IP. System współpracuje ze standardowymi serwerami, nośnikami danych oraz stacjami roboczymi. Jest też skalowany, co oznacza, że może być swobodnie rozbudowywany wraz ze wzrostem potrzeb. VMS będzie integrowany także z systemem automatyki budynkowej Building Integration System (BIS). Pozwala to na przykład na wyświetlanie obrazu bieżącego z określonych kamer w przypadku alarmu wyzwolonego przez BIS, uruchamianie lub zatrzymywanie zapisu obrazu z określonych kamer lub wyszukiwanie obrazów związanych z alarmem systemu BIS.

System umożliwia przypisanie praw dostępu do określonych kamer, funkcji sterowania kamerami, praw eksportu obrazów oraz dostępu do plików rejestru określonym grupom operatorów.

System pozwala na tworzenie elastycznych harmonogramów zapisu dla każdej kamery. Dzięki temu można uzyskać zapis z określoną częstotliwością odświeżania w ciągu dnia, w porze nocnej lub w okresie weekendu oraz zaprogramować ustawienia specjalne na czas świąt czy dni wolnych. Każdą z kamer można skonfigurować na minimalny i maksymalny czas przechowywania zarejestrowanych obrazów. System umożliwia również monitorowanie i zapis kanałów audio.

Opcja nadmiarowości rejestracji umożliwia kontynuowanie zapisu dla dowolnej kamery, podczas gdy na centralnym serwerze jest przechowywana historia lokalizacji zapisów. Kamery, komputery, oprogramowanie oraz sieć są stale kontrolowane przez system VMS.

W sytuacji alarmowej najważniejsza jest jak najszybsza reakcja, gdyż to ona decyduje o bezpieczeństwie chronionych osób lub mienia. Dlatego system VMS został tak zaprojektowany, aby zapewnić łatwą identyfikację i obsługę zdarzeń o najwyższym priorytecie. Alarmy mogą być sterowane harmonogramem i zostać indywidualnie przypisane do określonych grup operatorów. Nagranie ze zdarzeniem alarmowym jest wyświetlane w specjalnym oknie alarmów, dzięki czemu operatorzy nie muszą przeszukiwać ekranów w poszukiwaniu zarejestrowanych obrazów.

Dzięki wykorzystaniu technik zawartości obrazu system VMS zapewnia natychmiastową identyfikację najważniejszych zdarzeń. Przykładem może być zaawansowana detekcja ruchu, która umożliwia zidentyfikowanie wielkości obiektu, a także prędkości i kierunku jego poruszania się. Pozwala to rozpoznać takie zdarzenie, jak wejście lub wyjście obiektu z wyznaczonego obszaru oraz wykryć nieruchome obiekty, a tym samym zapobiec wystąpieniu zdarzenia alarmowego.

Zaawansowane funkcje linii czasu pozwalają na łatwe wyszukiwanie fragmentów zapisu, a opcje inteligentnego wyszukiwania pozwalają zobaczyć materiał zarejestrowany podczas zdarzenia przez poszczególne kamery. Dzięki możliwości wyświetlenia wielu

obrazów w tym samym czasie możliwy jest podgląd na żywo, a jednocześnie przeglądanie zapisanych danych.

Klawiatura może być dołączona do odbiornika sieciowego, co umożliwia wybór kamery na wszystkich monitorach analogowych, sterowanie sekwencją kamer oraz pełne sterowanie funkcjami obrotu, pochylenia i zoomu.

7. Instalacja nagłośnienia

Projektowany system jest systemem nagłośnienia trybun stadionu miejskiego w Radomiu. System ma za zadanie dostarczyć klarowny i zrozumiały przekaz komentarza sportowego, oraz wysokiej jakości muzyki towarzyszącej zawodom.

Instalacja systemu będzie podzielona na etapy, gdzie w każdym z etapów system musi być optymalnie skonstruowany tak, aby możliwie najniższym kosztem następowała rozbudowa o kolejny etap.

System nagłośnienia trybun ma spełniać dwa podstawowe zadania:

- Przekaz komentarza sportowego, oraz muzyki towarzyszącej zawodom sportowym.
- Przekaz komunikatu alarmowego celem przeprowadzenia sprawnej akcji ewakuacyjnej ze stadionu.

System informacyjny wewnątrz budynku ma za zadanie:

- przekazywanie reklam, informacji, a także sygnału z komentatora sportowego nadawanego na trybuny.

7.1. Specyfikacja ogólna systemu

Lp.	Parametr	Wartość	Uwagi
1	Ilość zestawów głośnikowych do nagłośnienia trybun	63 4	Trybuny Boisko
2	Kąt zasięgu zestawów głośnikowych do nagłośnienia trybun – urządzenia główne	90°H x 40°V 60°H x 60°V	
3	Użyteczny zakres częstotliwości zestawów głośnikowych do nagłośnienia trybun	85 Hz - 16 kHz	
6	Stopień ochrony zestawów głośnikowych	IP55	
7	Rodzaj transmisji sygnału pomiędzy punktami rozproszonymi systemu	Sieciowa, po sieci Ethernet	Protokół DANTE.
10	Opóźnienie sygnału audio dla transmisji sieciowej pomiędzy punktami rozproszonymi systemu. Od wejść analogowych matrycy na stanowisku komentatora do wyjść analogowych	<4ms	Teoretyczna suma opóźnień poszczególnych elementów toru oraz sieci przesyłu sygnału.

Lp.	Parametr	Wartość	Uwagi
	matryc w amplifikatorniach.		
11	Ilość kanałów transmisji bezprzewodowej – mikrofony	2	-
12	Ilość przewodowych mikrofonów na stanowisku komentatora sportowego	1	-
15	Ilość punktów rozproszonych systemu	3	2 x amplifikatornia oraz stanowisko komentatora w sieci Dante
16	Ilość pierścieni sieci światłowodowej	1	
17	Ilość kanałów w konsolcie fonicznej na stanowisku komentatora sportowego.	24	W tym min 4 stereo.
21	Poziom ciśnienia akustycznego z charakterystyką korekcyjną C dla trybun. Głośnikiysterowane sygnałem o ich mocy znamionowej i widmie szumu różowego.	$\geq 102\text{dB}$	+/- 3dB Na powierzchni min. 95%.
23	Wskaźnik zrozumiałości mowy na trybunach wyrażony parametrem STIPA przy 100 % wypełnieniu trybun publicznością i poziomie zakłóceń z tabeli 1a. Głośnikiysterowane sygnałem o mocy nie większej od ich mocy znamionowej i widmie szumu różowego.	$\geq 0,50$	Kategoria G wg PN-EN 60268-16:2011 Na powierzchni min. 95%.

7.2. Specyfikacja szczegółowa urządzeń głośnikowych

Zestaw głośnikowy nagłośnienia trybun ZG – A:

PARAMTER	WARTOŚĆ
Typ	Dwudrożny
Pasmo przenoszenia	85Hz to 16 kHz
Skuteczność (80 Hz - 16 KHz)	100dB
Skuteczność(250Hz - 4000Hz)	101dB
Nominalny kąt zasięgu (-6dB)	90° H 40° V
Moc znamionowa	200W
Współczynnik kierunkowości osiowy Q	>18
Waga	16,8kg
Stopień ochrony	IP55 (zgodnie z IEC529)
Budowa	Tworzywo sztuczne, LLDPE, osprzęt ze stali nierdzewnej. Grill potrójny WaterStop.

PARAMTER	WARTOŚĆ
Typ	Dwudrożny
Sposób mocowania	5 otworów z gwintem. Fabryczny uchwyt lub/i dedykowana konstrukcja do montażu do dźwigarów.

Zestaw głośnikowy nagłośnienia trybun ZG – B:

PARAMTER	WARTOŚĆ
Typ	Dwudrożny
Pasma przenoszenia	85Hz to 16 kHz
Skuteczność (80 Hz - 16 KHz)	102dB
Skuteczność(250Hz - 4000Hz)	102dB
Nominalny kąt zasięgu (-6dB)	60° H 60° V
Moc znamionowa	200W
Współczynnik kierunkowości osiowy Q	>21
Waga	16,8kg
Stopień ochrony	IP55 (zgodnie z IEC529)
Budowa	Tworzywo sztuczne, LLDPE, osprzęt ze stali nierdzewnej. Grill potrójny WaterStop.
Sposób mocowania	5 otworów z gwintem. Fabryczny uchwyt lub/i dedykowana konstrukcja do montażu do dźwigarów.

Zestaw głośnikowy nagłośnienia boiska ZGB:

PARAMTER	WARTOŚĆ
Typ	Trójdrożny
Pasma przenoszenia	70 Hz to 16 kHz
Skuteczność 1W / 1m	107 dB
Skuteczność 2,83V / 1m	110 dB
Nominalny kąt zasięgu (-6dB)	50° H 20° V
Moc znamionowa	400W
Poziom maksymalny / peak	133dB / 139dB
Waga	>47 kg
Stopień ochrony	IP55 (zgodnie z IEC529)
Budowa	Laminat szklano epoksydowy, osprzęt ze stali nierdzewnej. Grill potrójny WaterStop.

PARAMTER	WARTOŚĆ
Typ	Trójdrożny
Sposób mocowania	5 otworów z gwintem. Fabryczny uchwyt lub/i dedykowana konstrukcja do montażu do dźwigarów.
Dodatkowe informacje	Dedykowany transformator wysokiej klasy 400W/100V

Zestaw głośnikowy ścienny typ 1:

PARAMTER	WARTOŚĆ
Pasma przenoszenia	60 Hz - 22 kHz
Skuteczność (125 Hz to 12.5 kHz)	95dB
Skuteczność(250hz-4000hz)	96dB
Nominalny kąt zasięgu	115° stożkowo (+46° / -46°, 500 Hz to 6 kHz)
Moc znamionowa	120W, 60W, 30W / 100V
Współczynnik kierunkowości osiowy Q/DI	5.7 / 7.6, 500 Hz to 6 kHz
Waga	8,3kg.
Stopień ochrony	IP55 (zgodnie z IEC529)
Sposób mocowania	Dedykowany uchwyt kulowy

Zestaw głośnikowy sufitowy podwyższonej jakości:

PARAMTER	WARTOŚĆ
Pasma przenoszenia	90 Hz - 18.5 kHz
Skuteczność (160 Hz to 12.5 kHz)	92dB
Skuteczność(250hz-4000hz)	93dB
Nominalny kąt zasięgu	130° stożkowo(1 Hz to 6 kHz) 140° stożkowo (500 Hz to 6 kHz)
Moc znamionowa	60W; 30W, 15W, 7.5W/100V
Współczynnik kierunkowości osiowy Q/DI	4 / 6, 500 Hz to 6 kHz
Waga	3kg
Sposób mocowania	Montaż w suficie podwieszanym

Zestaw głośnikowy typu projektor:

PARAMTER	WARTOŚĆ
Pasma przenoszenia	75 Hz - 20 kHz
Skuteczność (1KHz/1m/1W)	86 dB (SPL)
Nominalny kąt zasięgu	220° / 65°
Moc znamionowa	10 / 5 / 2,5 W
Waga	3kg
Sposób mocowania	Dedykowany uchwyt

Zestaw głośnikowy sufitowy:

PARAMTER	WARTOŚĆ
Pasmo przenoszenia	100Hz – 20 000Hz
Skuteczność (80 Hz to 16 KHz)	97dB
Nominalny kąt zasięgu (-10dB)	180°
Moc znamionowa	6W
Waga	1,15kg
Sposób mocowania	Montaż w suficie podwieszanym.

7.3. Okablowanie

7.3.1. Okablowanie głośnikowe

Do zestawów głośnikowych należy prowadzić okablowanie głośnikowe o przekroju min $2 \times 6 \text{ mm}^2$. W przypadku krótszych linii głośnikowych zweryfikować na etapie wykonawstwa możliwość zastosowania mniejszych przekroi. Okablowanie prowadzić możliwymi dostępnymi trasami kablowymi.

7.3.2. Okablowanie sygnałowe

NAZWA TRASY	SKĄD	DOKĄD	TYP KABLA
LS01	STANOWISKO KOMENTATORA	SZAFRA RACK - GŁÓWNA	ŚWIATŁOWÓD DWA WŁÓKNA
LS02	SZAFRA RACK - GŁÓWNA	SZAFRA RACK - POMOCNICZA	ŚWIATŁOWÓD DWA WŁÓKNA
LS03	SZAFRA RACK - POMOCNICZA	STANOWISKO KOMENTATORA	ŚWIATŁOWÓD DWA WŁÓKNA
LS04	STANOWISKO KOMENTATORA	POMIESZCZENIE POLICJI	CAT 5e
LS05	STANOWISKO KOMENTATORA	SYSTEM SAP	CAT 5e

8. Instalacje teleinformatyczne (okablowanie strukturalne)

Projekt sieci LAN obejmuje system w oparciu o przewód kat. 7, cała instalacja o klasie wydajności E_A.

Punkty sieciowe zostaną zaprojektowane w miejscach (pomieszczeniach) wymienionych w PFU, przy punktach kamerowych, innych urządzeniach teletechnicznych pracujących w sieci strukturalnej.

8.1. Wymagania podstawowe:

- ilość i lokalizację stanowisk (punktów końcowych), przyjęto na podstawie aktualnych dla daty wykonywania dokumentacji podkładów architektonicznych,
- w przypadku zmiany tej koncepcji, ostateczna i precyzyjna lokalizacja gniazd logicznych powinna być ustalona między Użytkownikiem, a

Wykonawcą w trakcie realizacji,

- wszystkie elementy pasywne (miedziane i światłowodowe, kable instalacyjne, panele, gniazda, kable krosowe) składające się na okablowanie strukturalne muszą być trwale oznaczone nazwą lub znakiem firmowym producenta i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu gwarancyjnego producenta,
- maksymalna długość kabla instalacyjnego (S/FTP) w łączy stałym (od punktu dystrybucyjnego do gniazda końcowego) nie może przekroczyć 90 metrów, zgodnie z poniższym rys. przedstawiającym segmenty sieci,
- projekt wymaga zastosowania kabla miedzianego okablowania poziomego o wyższej niż opisana wydajności, celem zapewnienia Użytkownikowi zapasu transmisyjnego dla nowych usług i standardów transmisyjnych,
- wszystkie komponenty powinny charakteryzować się pełną zgodnością ze specyfikacją dla minimum kategorii 6_A (zgodnie z normą PN-EN 50173-1: 2011 oraz ISO 11801 2nd edition: 2002 Amd 2 2010),
- zgodność parametrów modułów gniazd z obowiązującymi normami minimum kategorii 6_A musi odpowiadać wymaganiom Normy międzynarodowej, tj. ISO/IEC 11801:2011 oraz europejskiej tj. EN 50173-1 i być na etapie oferty potwierdzona poprzez przedstawienie certyfikatów wydanych przez akredytowane niezależne laboratoria (np. GHMT, 3P, Delta) potwierdzające zgodność systemu / komponentu z wymaganiami Normy międzynarodowej, tj. ISO/IEC 11801:2011. W przypadku dokumentów wystawionych przez inne niż wskazane akredytowane laboratoria certyfikujące, wymagane jest posiadanie przez tą instytucję akredytację typu AC (lub równoważnej) jednostki nadrzędnej w danym kraju (np. w Polsce jednostka nadrzędna to Polskie Centrum Akredytacji),
- skrzętka teleinformatyczna musi posiadać minimum jeden certyfikat niezależnego instytutów badawczych (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2((2011-06)), IEC 61156-5 Ed.2.1 (2012-12)} dla potwierdzenia spełniania parametrów.
- moduł RJ45 Keystone JACK musi posiadać minimum dwa certyfikaty dwóch niezależnych instytutów badawczych (GHMT, 3P, DELTA) w zgodności z normami {ISO/IEC 11801 ED.2.2((2011-06)), EN 50173-1((2011-11)), ANSI/TIA-568-C.2 ((2009-08))} dla potwierdzenia spełniania parametrów,
- wydajność systemu okablowania (Permanent Link) musi być potwierdzona certyfikatem przynajmniej jednego niezależnego akredytowanego laboratorium, np. GHMT, DELTA, itp. Certyfikaty muszą obejmować wszystkie aktualne normy okablowania normami {ISO/IEC 11801 ED.2.2((2011-06)), EN 50173-1((2011-09)), ANSI/TIA-568-C.2 ((2009-08))},
- wymóg posiadania powyższych certyfikatów jest uzasadniony z punktu

widzenia gwarancji jakości i powtarzalności najwyższych parametrów komponentów i całego systemu,

- system okablowania strukturalnego powinien być objęty 25 letnią gwarancją systemową wystawianą przez producenta (gwarancja na szafy minimum 5 lat).

8.2. Specyfikacja techniczna urządzeń instalacji okablowania strukturalnego

8.2.1. Przewód światłowodowy

Okablowanie szkieletowe będzie prowadzone FO z 12 włóknami.

8.2.2. Przewód typu skrętka

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

Kabel musi posiadać trwałe rozróżnienie kolorystyczne dedykowane dla kategorii.

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

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

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

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

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

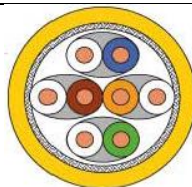
Charakterystyka kabla ma uwzględniać odpowiedni margines pracy, tj. pozytywne parametry transmisyjne do min.690MHz dla kabla kat.7.

WYMAGANE PARAMETRY KABLA TELEINFORMATYCZNEGO

Opis konstrukcji:

Opis	Kabel S/FTP (PiMF) 695 MHz
Zgodność z normami	ISO/IEC 11801:2002 wyd. II, ISO/IEC 61156-5:2002, EN 50173-1:2011, EN 50288-3-1, TIA/EIA 568-B.2

	(parametry kategorii 7), IEC 60332-1, IEC 60754-2; IEC 61034
Średnica przewodnika	drut 23 AWG (Ø 0,56 mm)
Liczba par kabla	4 (8 przewodów)
Średnica zewnętrzna kabla	6,9 mm
Minimalny promień gięcia	30mm
Waga	50,2 kg/km
Temperatura pracy	-20°C do +60°C
Temperatura podczas instalacji	0°C do +50°C
Ośłona zewnętrzna	FRNC
Ekranowanie par	laminowana folia aluminiowa
Ogólny ekran	plecionka miedziana, cynowana



Rys. Przekrój kabla S/FTP (PiMF)

Charakterystyka elektryczna – wartości typowe:

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

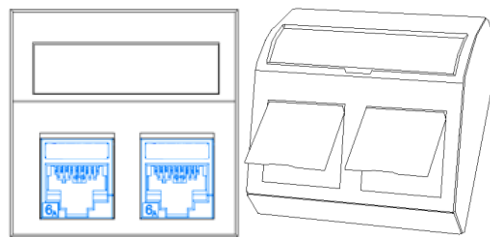
8.2.3. Punkt logiczny (PL)

Punkt logiczny PL oparty został na płycie czołowej skośnej (kątowej, z wyprowadzeniem kabli przyłączeniowych na dół, na skos, od strony ściany zaś pionowo, do góry kabla instalacyjnego – w celu zagwarantowania najbardziej łagodnego prowadzenia kabli, a także zabezpieczenia przed ich załamaniem pod wpływem własnego ciężaru lub przez monterów podczas instalacji). Płyta czołowa ma posiadać klapki przeciw-

kurzowe oraz w górnej części, widocznej dla Użytkownika, pola pozwalające na wprowadzenie oddzielnego każdego modułu gniazda (numeracji portu), przy czym opisy te muszą być zabezpieczone przezroczystymi pokrywami (chroniącymi przed zamazaniem lub zabrudzeniem). Płyta czołowa ma być zgodna ze standardem uchwyty typu Mosaic (45x45mm), celem jak największej uniwersalności i możliwości adaptacji do dowolnego systemu i linii wzorniczej osprzętu elektroinstalacyjnego dowolnego producenta.

8.2.4. Adapter kątowy 2xRJ45 (45x45)

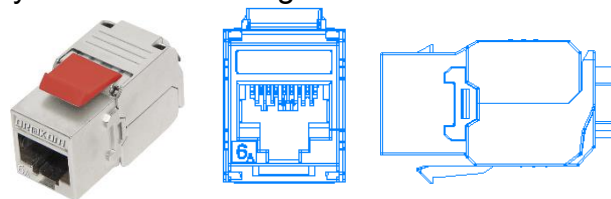
Punkt logiczny należy zbudować w oparciu o płytę czołową kątową. Płyta czołowa ma posiadać klapy/osłonki przeciw kurzowe oraz (w celach opisowych) w górnej części, widocznej dla Użytkownika, pole pozwalające na wprowadzenie opisu każdego modułu gniazda (numeracji portu) – przy czym opisy muszą być zabezpieczone przezroczystymi pokrywami (chroniącymi przed zamazaniem lub zabrudzeniem). Płyta czołowa ma być zgodna ze standardem uchwyty typu Mosaic (45x45mm).



Rys. Przykładowy widok adaptera kąтового 2M

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

8.2.5. Ekranowany moduł RJ45 kategorii 6A



Rys. Ekranowany moduł RJ45 kat. 6A

Minimalne parametry produktu:

Moduły RJ45 musi być wykonany w standardzie Keystone Jack, co pozwala na ich montaż w każdym dostępnym osprzęcie. Moduł RJ45 powinien zapewnić uniwersalność rozwiązania (taki sam moduł po stronie gniazda i po stronie panela krosowego modułarnego).

Moduł RJ45 musi posiadać możliwość zrobienia zarówno beznarzędziowego jak i narzędziowy oraz wielokrotnego użytku - pozwalając na demontaż z kabla skrętkowego a następnie powtórne zaterminowanie.

Moduł RJ45 musi posiadać trwałe oznaczenie kategorii dla której jest dedykowany, logo

producenta i logo systemu.

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

Przynajmniej jeden z certyfikatów musi potwierdzać spełnianie następujących norm i standardów: IEC 60603-7-51, IEC 60512-27-100, ANSI/TIA 568-C.2, oraz potwierdzać spełnienie procedury badawczej RE-EMBEDDED.

8.2.6. Modularny panel krosowy 24xRJ45 1U

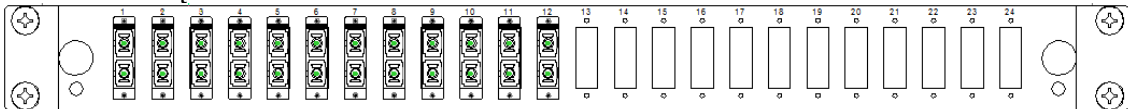


Rys. modularny panel krosowy 24xRJ45 1U

Kable należy zakończyć na 19", modularnym 24xRJ45, ekranowanym panelu krosowym. Panel musi posiadać max. wysokość 1U oraz możliwość zamontowania 24 ekranowanych modułów typu Keystone RJ45 Kat.6A.

Panele krosowe muszą posiadać trwałe oznaczenie logo producenta i logo systemu oraz pole opisowe. Panel musi posiadać zintegrowaną półkę kablową umożliwiającą przymocowanie kabli za pomocą opasek. Metalowa konstrukcja zapewnia galwaniczne połączenie z ekranami modułów. Panel musi posiadać możliwość podłączenia przewodu uziemienia.

8.2.7. Przełącznica światłowodowa



Rys. Przykładowy widok przełącznicy światłowodowej

Panel krosowy światłowodowy 1U obsługuje do 24 x SC duplex.

Kolor przełącznicy musi być zgodny i jednolity z całością systemu okablowania w części miedzianej.

Przełącznica musi posiadać dwie płaszczyzny wysuwania, 5 wejść kabla od tyłu, możliwość instalacji dławików kablowych, oraz organizatorów przednich. Panel ma zapewnić zamontowanie 4 kaset światłowodowych.

Producent musi posiadać w swojej standardowej ofercie kompletne rozwiązania światłowodowe obejmujące cały tor transmisji tj. kabel krosowy o dowolnym interfejsie, adaptory i pigtaile światłowodowe (SC, LC, LCQUAD, ST, MTRJ, E2000, FC), tacki i osłonki spawów oraz elementy zaślepiające porty przełącznicy optycznej.

8.2.8. Szafy dystrybucyjne

GPD – Główny Punkt Dystrybucyjny, szafy 42U 800x1000, połączenie z GPD w obszarze hali, połączenie z punktami PPD w obszarze stadionu.

PPD – Pośrednie Punkty Dystrybucyjne, szafy 42U 800x800, połączenie z GPD w obszarze stadionu.

8.3. Administracja i dokumentacja

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, tak od strony gniazda, jak i od strony szafy montażowej. Te same oznaczenia należy umieścić w sposób trwały na gniazdach sygnałowych w punktach przyłączeniowych Użytkowników oraz na panelach.

Powykonawczo należy sporządzić dokumentację instalacji kablowej uwzględniając wszelkie, ewentualne zmiany w trasach kablowych i rzeczywiste rozmieszczenie punktów przyłączeniowych w pomieszczeniach. Do dokumentacji należy dołączyć raporty z pomiarów torów sygnałowych.

8.4. Odbiór i pomiary sieci

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest uzyskanie gwarancji systemowej producenta potwierdzającej weryfikację wszystkich zainstalowanych torów na zgodność parametrów z wymaganiami norm Klasy E_A / Kategorii 6_A wg obowiązujących norm.

W celu odbioru instalacji okablowania strukturalnego należy spełnić następujące warunki:

- Wykonać komplet pomiarów – opis pomiarów części miedzianej i światłowodowej.

Wykonawstwo pomiarów powinno być zgodne z normą PN-EN 50346:2004/A1+A2:2009. Pomiary sieci światłowodowej powinny być wykonane zgodnie z normą PN-EN 14763-3:2009/A1:2010. Pomiary należy wykonać dla wszystkich interfejsów okablowania poziomego oraz szkieletowego.

Należy użyć miernika dynamicznego (analizatora), który posiada wgrane oprogramowanie umożliwiające pomiar parametrów według aktualnie obowiązujących norm. Sprzęt pomiarowy musi posiadać aktualny certyfikat potwierdzający dokładność jego wskazań.

Analizator okablowania wykorzystany do pomiarów musi charakteryzować się przynajmniej IV klasą dokładności wg IEC 61935-1/Ed. 3 (proponowane urządzenia to np. Lantek 7G, FLUKE DTX 1800, PSIBER - WireXpert).

W przypadku sieci miedzianej pomiary należy wykonać w konfiguracji pomiarowej łącza stałego (ang. „Permanent Link”) – przy wykorzystaniu odpowiednich adapterów pomiarowych specyfikowanych przez producenta sprzętu pomiarowego

Pomiary należy skonfrontować z wydajnością klasy E_A specyfikowanej wg. ISO/IEC11801:2002/Am2:2010 lub EN50173-1:2011.

Pomiar każdego toru transmisyjnego poziomego (miedzianego) powinien zawierać:

- ✓ Attenuation – (Insertion Loss)
- ✓ NEXT - Near-End X-Talk
- ✓ ACR-N - Attenuation-to-Crosstalk Ratio NEXT;
- ✓ PS NEXT - PowerSum NEXT
- ✓ PS ACR-N - PowerSum ACR-N

- ✓ ACR-F - Attenuation-to-Crosstalk Ratio FEXT; dawniej ELFEXT – Equal Level FEXT
- ✓ PS ACR-F - PowerSum ACR-F; dawniej PS ELFEXT
- ✓ RL – Return Loss

Tłumienie światłowodowego toru transmisyjnego może być wyznaczone za pomocą miernika spadku mocy optycznej lub reflektometru.

Niezależnie od użytego sprzętu pomiarowego kompletny pomiar tłumienia każdego dwupleksowego toru transmisyjnego powinien być przeprowadzony w dwie strony w dwóch oknach transmisyjnych dla dwóch włókien (chyba że typ złącza uniemożliwia taką procedurę):

- od punktu A do punktu B w oknie 850nm i 1300nm (MM),
- od punktu B do punktu A w oknie 850nm i 1300nm (MM),

Na raportach pomiarów powinna znaleźć się informacja opisująca wielkość marginesu (inaczej zapasu, tj. różnicy pomiędzy wymaganiem normy a pomiarem, zazwyczaj wyrażana w jednostkach odpowiednich dla każdej mierzonej wielkości).

Zastosować się do procedur certyfikacji producenta systemu okablowania strukturalnego.

8.5. Wymagania dla instalatora

Instalacja okablowania strukturalnego musi zostać wykonywana przez instalatora posiadającego ważne uprawnienia i certyfikat wydany przez producenta okablowania (certyfikowany instalator systemu). Zaleca się, aby wykonawca posiadał również ważny status certyfikowanego projektanta systemu ze względu na procedurę gwarancyjną – projekt powykonawczy.

Uprawnienia certyfikowanego instalatora systemu muszą obejmować wszystkie stopnie/poziomy kwalifikacji: instalację, nadzór, serwis i kwalifikowanie do objęcia gwarancją niezawodności. Certyfikat musi być wystawiony przez producenta systemu okablowania. Nie dopuszcza się certyfikatu wystawionego przez dystrybutora, reselera, czy innego przedstawiciela nie będącego producentem. Certyfikat powinien być wystawiony w języku polskim; posiadać nazwę instalatora (firmy), nazwisko instalatora, zakres uprawnień oraz datę wystawienia certyfikatu.

Wykonawca autoryzujący system okablowania strukturalnego musi posiadać uprawnienia do objęcia zainstalowanego systemu co najmniej 25-letnią systemową gwarancją niezawodności, udzielaną przez producenta okablowania.

8.6. Wymagania gwarancyjne

Wykonawca jest zobowiązany do dostarczenia aktualnej dokumentacji powykonawczej w postaci elektronicznej (wersja edytowalna tj pliki .dwg, .doc, excel, oraz nieedytowalne tj. .pdf) jak i w formie papierowej z pomiarami sieci logicznej i elektrycznej.

Całość procedury jest opisana w dokumencie „Gwarancja Systemowa. Certyfikowany System Okablowania Strukturalnego”.

Po zakończeniu instalacji, Wykonawca wystąpi z wnioskiem do Producenta Okablowania o certyfikację instalacji kategorii 6A i po pozytywnie zakończonym

audycie, dostarczy „Certyfikat” Użytkownikowi.

Gwarancja Systemowa na Certyfikowany System Okablowania Strukturalnego obejmuje:

- Gwarancję produktową - Wszystkie komponenty Certyfikowanego Systemu Okablowania Strukturalnego będą wolne od wad materiałowych i wad wykonania pod warunkiem ich prawidłowego montażu i eksploatacji,
- Gwarancję wydajności - Parametry łącza stałego lub kanału Certyfikowanego Systemu Okablowania Strukturalnego będą spełniać wymogi określone przez normy ISO/IEC 11801, EN 50173, PN-EN 50173-1, TIA/EIA 568A/B dla klasy wydajności, dla której łącze było zaprojektowane,
- Gwarancję na pracę aplikacji - Gwarancja nie jest ograniczona poprzez definiowane z góry poszczególnych protokołów transmisji możliwych do zastosowania przez Użytkownika. Certyfikowany System Okablowania Strukturalnego będzie umożliwiał transmisję sygnałów w oparciu o protokoły i aplikacje sieciowe zdefiniowane przez komitety normalizacyjne IEEE, ANSI, TIA/EIA oraz ATM Forum i zatwierdzonych do transmisji w oparciu o aktualne normy ISO/IEC 11801, EN 50173 , PN-EN 50173-1, TIA/EIA 568A/B.

Gwarancja Systemowa – procedura uzyskania gwarancji

- Pierwszym etapem procedury uzyskania Gwarancji Systemowej jest przesłanie do producenta okablowania wypełnionego Formularza Zgłoszeniowego przed rozpoczęciem instalacji,
- Formularz Zgłoszeniowy zawiera podstawowe informacje dotyczące instalacji, Certyfikowanego Instalatora oraz terminów rozpoczęcia i zakończenia instalacji,
- Producent zastrzega sobie możliwość kontroli instalacji podczas jej realizacji, jak również po jej zakończeniu,
- Po wykonaniu instalacji do Producenta Systemu należy dostarczyć następujące dokumenty:
 - Podpisany i ostemplowany komplet dokumentacji powykonawczej zawierającej schemat ideowy instalacji oraz projekty punktów dystrybucyjnych (szaf),
 - Listę zainstalowanych komponentów wraz z kopiami faktur zakupowych,
 - Wyniki pomiarów dynamicznych torów miedzianych łączy stałych lub kanałów (Permanent Link) oraz wyniki pomiarów tłumienia torów światłowodowych wykonanych według obowiązujących norm ISO/IEC 11801 lub EN 50173-1. Pomiary światłowodowe muszą być wykonane w dwóch oknach, w dwóch kierunkach. Należy wykonać przynajmniej pomiar tłumienności kanału.
 - Pomiary muszą być dostarczone w formacie elektronicznym

- miernika (.flt, .fcm, .dat, .mdb itp.),
 - Załączyć należy aktualne świadectwo kalibracji miernika użytego do wykonania pomiarów,
- W przypadku stwierdzenia nieprawidłowości w wykonanej instalacji, Certyfikowany Instalator wykonuje niezbędne poprawki i zgłasza je do Producenta Systemu, po czym ustalany jest termin kontroli sieci (kontrola ta może być odpłatna),
- Po potwierdzeniu właściwego wykonania instalacji przez Producenta Systemu wystawiona zostanie nieodpłatnie Gwarancja Systemowa na Certyfikowany System Okablowania Strukturalnego w postaci certyfikatu.
- Wykonać należy dokumentację powykonawczą, która ma zawierać:
 - Raporty z pomiarów dynamicznych okablowania,
 - Rzeczywiste trasy prowadzenia kabli transmisyjnych poziomych,
 - Oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych,
 - Lokalizację przebiegów przez ściany i podłogi.
- Raporty pomiarowe wszystkich torów transmisyjnych należy zawrzeć w dokumentacji powykonawczej i przekazać inwestorowi przy odbiorze inwestycji. Drugą kopię pomiarów (dokumentacji powykonawczej) należy przekazać producentowi okablowania w celu udzielenia Inwestorowi (Użytkownikowi końcowemu) bezpłatnej gwarancji.

8.7. Uwagi końcowe

Wszystkie szafy dystrybucyjne muszą być uziemione by zapobiec powstawaniu zakłóceń. Dedykowaną dla okablowania instalację elektryczną należy wykonać zgodnie z obowiązującymi normami i przepisami.

Wszystkie materiały wprowadzone do robót winny być nowe, nieużywane, najnowszych aktualnych wzorów, winny również uwzględniać wszystkie nowoczesne rozwiązania techniczne.

9. System sprzedaży i kontroli biletów z identyfikacją kibiców

9.1. Przedmiot i zakres opracowania

Projektowany system dla Hali Sportowo Widowiskowej oraz Stadionu Piłkarskiego w Radomiu będzie pracował w oparciu o jedną bazę danych i będzie się składać z następujących modułów:

- a) Budowania i Zarządzania Bazą Klientów wraz z aplikacją do rejestracji mediów i wydawania akredytacji
- b) Sprzedaży Dokumentów Wejściowych, Produktów i Usług (wraz z modułem fakturowania)
- c) Zarządzania Grafikiem Rezerwacji Zasobów, Obiektów i Usług
- d) Administracyjnego
- e) Kontroli Wejścia i Identyfikacji Kibiców wraz z modułem obsługi

9.2. Podstawa opracowania

Projekt powstał w oparciu o następujące normy i obowiązujące przepisy, a dostarczony System i wykonane prace będą w pełni zgodne z tymi normami i przepisami:

- a) ustawę o bezpieczeństwie imprez masowych z dnia 20 marca 2009 r. (Dz. U. Nr 62 poz. 504 z 2009 r) wraz z późniejszymi zmianami,
- b) wytyczne UEFA i FIFA,
- c) uchwałę nr XIV/191 z dnia 28.11.2007 r. Zarządu PZPN w sprawie niektórych wymagań technicznych dla lokalizacji i budowy nowych stadionów,
- d) CBDK PZPN-u,
- e) System Centralny Kibic spółki Ekstraklasa,
- f) ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. Nr 133, poz. 883) wraz z późniejszymi zmianami,
- g) rozporządzenie MSWiA z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz.1024),
- h) ustawę o świadczeniu usług drogą elektroniczną,
- i) ustawę o rachunkowości.

9.3. Wytyczne realizacyjne

Prawidłowe wdrożenie systemu obejmować będzie czynności mające na celu dostarczenie, konfigurację i uruchomienie Systemu, świadczenie opieki gwarancyjnej, w tym w szczególności:

- a) Przeprowadzenie analizy przedwdrożeniowej z Inwestora,
- b) Dostawę, montaż i konfigurację wszystkich urządzeń i infrastruktury sprzętowej Systemu,
- c) Instalację i konfigurację Oprogramowania Systemu,
- d) Przeprowadzenie szkoleń dla osób wskazanych przez Inwestora,
- e) Konfigurację i uruchomienie Systemu,
- f) Wprowadzenie graficznej mapy obiektu przekazanej przez Inwestora, planu trybun, sektorów, poszczególnych miejsc.

Szkolenia dla Administratorów/Menedżerów systemu będą prowadzone w grupie maks. 3 osobowej, dla sprzedawców/kasjerów w 2 grupach maks. 12 osobowych, aby zapewnić najwyższą efektywność prowadzonych szkoleń.

Szkolenie dla sprzedawców/kasjerów w punktach sprzedaży/obsługi klienta będą trwać 8 godzin dla każdej z 2 grup i obejmować będą wszystkie procesy realizowane w

Systemie związane z obsługą klienta w punkcie sprzedaży dotyczące jego rejestracji (założenia profilu), identyfikacji osób, sprzedaży dokumentów wejściowych oraz innych produktów i usług dostępnych na obiekcie, stornowania dokumentów wejściowych, rozpatrywania reklamacji, wystawiania faktur, obsługi depozytu, realizowania rozliczeń i raportów kasjerskich, obsługi urządzeń wchodzących w skład wyposażenia stanowiska kasjerskiego.

Szkolenia dla Administratorów/Menedżerów Systemu ze względu na bardzo duży zakres wiedzy będą odbywały się w dwóch cyklach realizowanych w odstępach czasu umożliwiających ugruntowanie i przeciwiczenie w praktyce wiedzy pozyskanej w danym cyklu oraz możliwość powtórzenia danego zakresu materiału w kolejnym cyklu oraz zadania pytań pojawiających się na etapie ćwiczeń i eksploatacji Systemu. Szkolenia będą obejmować 32 godziny szkoleniowe, w tym 24 godzin szkolenia podstawowego oraz 8 godzin szkolenia przypominającego.

Na hali sportowo – widowiskowej oraz na stadionie rozgrywane będą przede wszystkim imprezy masowe, w związku z tym dostarczany System będzie przystosowany do użytkowania zgodnie z aktualną ustawą o Bezpieczeństwie Imprez Masowych (BIM).

Eksploatacja systemu

Po końcowym Odbiorze Systemu i przekazaniu go do użytkowania Wykonawca będzie realizował następujące usługi:

- a) asyst technicznych na pierwszych 3 imprezach
- b) zdalnego wsparcia eksploatacyjnego Użytkownika w ciągu pierwszych 2 miesięcy od rozpoczęcia eksploatacji Systemu w wydłużonych godzinach od poniedziałku do piątku od 8-20 w soboty i niedziele od 12-18, a w czasie trwania imprez masowych w okresie wsparcia eksploatacyjnego – na 2 godziny przed rozpoczęciem imprezy i w czasie trwania imprezy masowej aż do jej zakończenia
- c) Upgrade'y Oprogramowania Aplikacyjnego Systemu w okresie pierwszych 12 miesięcy eksploatacji
- d) Realizację 5 przeglądów konserwacyjnych Systemu 1 raz w roku w okresie gwarancyjnym

9.4. Definicje

Access Point – punkt dostępowy dla terminali przenośnych.

Administrator – osoba wskazana przez Inwestora lub Użytkownika Końcowego posiadająca uprawnienia do dokonywania modyfikacji w ustawieniach i konfiguracji Systemu.

Aktualizacja – dostarczanie i instalowanie uaktualnień lub nowych wersji Oprogramowania Aplikacyjnego. Aktualizacja obejmuje udzielenie lub zapewnienie Inwestora licencji na korzystanie z nowych wersji Oprogramowania Aplikacyjnego oraz wdrożenie Aktualizacji przez okres 12- miesięcy od oddania Systemu.

Asysta Techniczna – usługa świadczona przez Wykonawcę polegająca na wsparciu pracowników Inwestora przy uruchamianiu Systemu na pierwszych imprezach odbywających się na obiektach z wykorzystaniem Systemu. Obejmuje przygotowanie Systemu do eksploatacji przed imprezą, wsparcie w monitorowaniu pracy Systemu w czasie eksploatacji - przed imprezą i w czasie jej trwania, wsparcie w poprawnym przygotowaniu statystyk i raportów z pracy Systemu oraz wyłączeniu Systemu po imprezie, a także bieżące rozwiązywanie pojawiających się problemów związanych z eksploatacją Systemu.

Dokumentacja Wdrożeniowa – dokumentacja powstająca w trakcie realizacji Wdrożenia, przede wszystkim na etapie uzgodnień analizy przedwdrożeniowej, obejmująca opis procesu dostosowania i konfiguracji Systemu do wymagań Inwestora (opis konfiguracji, parametryzacji i ustawień Systemu).

GPD – Główny Punkt Dystrybucyjny.

LAN – (Local Area Network) sieć strukturalna.

Oprogramowanie – Oprogramowanie Aplikacyjne Systemu Sprzedaży i Kontroli Biletów z Identyfikacją Kibiców.

Oprogramowanie Aplikacyjne – Oprogramowanie Systemu Sprzedaży i Kontroli Biletów z Identyfikacją Kibiców.

Oprogramowanie Narzędziowe – Oprogramowanie i licencje dostępne niezbędne do prawidłowego funkcjonowania Oprogramowania lub zarządzania zainstalowanymi urządzeniami lub do usprawniania i modyfikowania Oprogramowania Systemowego potrzebne do działania Systemu.

Oprogramowanie Osób Trzecich – Oprogramowanie wytworzone przez osoby inne niż Wykonawca, do którego osoby te posiadają autorskie prawa majątkowe.

Oprogramowanie Systemowe – odpowiednie Oprogramowanie i licencje dostępne realizujące funkcje niezbędne do uruchomienia i działania urządzeń, na których zostało zainstalowane.

PEL – Punkt Elektryczno-Logiczny.

PoE – (Power over Ethernet) zasilanie urządzenia za pomocą kabla UTP/SFTP.

Punkt Kontroli – stałe i/lub mobilne miejsce, w którym odbywa się elektroniczna kontrola uprawnień do wejścia/wyjścia do/z obiektu.

POK – Stanowisko Obsługi Klienta.

POS – (Point of Sale) Stanowisko Kasowe.

Punkt Sprzedaży – stacjonarne stanowisko kasowe - stanowisko sprzedaży umożliwiające w zależności od wyposażenia realizację funkcjonalności Systemu w zakresie obsługi Klienta/Kibica min.: rejestracji i weryfikacji profilu, sprzedaży produktów, usług i Dokumentów Wejściowych - należące do Inwestora lub Użytkownika Końcowego znajdujące się na stadionie (Wewnętrzny Punkt Sprzedaży) lub poza stadionem (Wyniesiony Punkt Sprzedaży) lub też znajdujące się poza stadionem i należące do podmiotu zewnętrznego (Zewnętrzny Punkt Sprzedaży).

System – System Sprzedaży i Kontroli Biletów z Identyfikacją Kibiców, spójna całość wszystkich wdrożonych elementów składających się na Przedmiot Zamówienia.

PPD – Pośredni Punkt Dystrybucyjny.

Upgrady Oprogramowania – nowe, standardowe wersje Oprogramowania wytworzone, wprowadzone i oferowane przez Producenta Oprogramowania. Upgrady nie obejmują modyfikacji i zmian Oprogramowania wykonywanych specjalnie na rzecz Inwestora lub Użytkownika Końcowego.

Użytkownik Końcowy – Użytkownik lub inny system informatyczny bezpośrednio eksploatujący System.

Wdrożenie Systemu – całokształt prac wykonanych przez Wykonawcę w celu umożliwienia samodzielnej eksploatacji Systemu przez pracowników Inwestora, a w szczególności takich czynności jak: dostawa, instalacja, konfiguracja Systemu, wykonanie testów weryfikacyjnych, konfiguracja i parametryzacja Systemu, opracowanie i dostarczenie Dokumentacji technicznej i dokumentacji dla Użytkownika Końcowego, szkolenie Użytkowników Końcowych i Administratorów, świadczenie usług Asysty Technicznej, świadczenie usług Wsparcia Eksploatacyjnego.

Wsparcie Eksploatacyjne – help-line - zdalna asysta techniczna świadczona przez Wykonawcę na rzecz Inwestora lub wskazanego przez niego Użytkownika Końcowego polegająca na rozwiązywaniu problemów pojawiających się przy eksploatacji Systemu oraz wyjaśnianiu wątpliwości Inwestora lub Użytkownika Końcowego związanych z eksploatacją Systemu.

9.5. Licencjonowanie

System będzie dostarczony wraz z niewyłączną, bezterminową licencją na korzystanie z oprogramowania zarządzającego systemu.

System będzie dostarczony wraz z wielostanowiskową licencją oprogramowania wystawioną na Inwestora, dla obiektu sportowego obejmującego halę sportowo-widowiskową i stadion piłkarski w Radomiu przy ul. Struga, dla:

- a) Nieograniczonej liczby Administratorów Inwestora
- b) Nieograniczonej liczby Punktów Sprzedaży
- c) Nieograniczonej liczby Punktów Kontroli
- d) Nieograniczonej liczby Użytkowników Inwestora i użytkowników sklepu www
- e) Nieograniczonej liczby wersji językowych sklepu www
- f) Nieograniczonej liczby Zewnętrznych Systemów Sprzedaży Biletów.

9.6. Opis ogólny systemu

System sprzedaży i kontroli biletów z identyfikacją kibiców będzie zapewniać kompleksową obsługę Klientów/Kibiców na hali sportowo - widowiskowej i stadionie piłkarskim w Radomiu w zakresie wszystkich procesów związanych z wejściem na biletowaną imprezę masową odbywającą się na obiekcie, skorzystaniem z produktów i usług oferowanych przez Inwestora lub Użytkownika obiektu dla Klientów/Kibiców w dniach imprez, ale też poza dniami imprez, w trakcie codziennego funkcjonowania

obiektu. System będzie umożliwiać zakup dokumentów wejściowych na imprezy w wewnętrznych i wyniesionych punktach sprzedaży, za pomocą zewnętrznych systemów sprzedaży biletów oraz w sklepie www, zgodnie z wymaganiami ustawy o Bezpieczeństwie Imprez Masowych.

System będzie gwarantować sprzedaż dokumentów wejściowych, produktów i usług w czasie rzeczywistym z jednoczesnym dostępem do wszystkich wolnych miejsc, stref, obiektów przez wszystkich sprzedawców i użytkowników sklepu www.

W przypadku imprez masowych odbywających się na obiekcie dokument wejściowy będzie umożliwiać przekroczenie określonego punktu kontrolnego prowadzącego do obiektu i zajęcie miejsca w określonym sektorze i rzędzie lub na wydzielonym sektorze. Kołowroty wejściowe wyposażone w zintegrowane sprawdzarki biletowe odczytujące kody kreskowe 1D i 2D, chipy RFID w standardzie MIFARE oraz czcionki OCR, będą porównywać dane zawarte na Dokumencie Wejściowym z danymi zawartymi w serwerze (Bazie Danych Systemu) lub pamięci wewnętrznej sprawdzarki biletowej i umożliwiać wejście do obiektu. Wszelkie nieprawidłowości w odczycie danych spowodują zablokowanie wejścia, odesłanie Klienta/Kibica do kasy reklamacyjnej lub punktu sprzedaży, pełniącego również funkcję kasy reklamacyjnej celem wyjaśnienia przyczyn nieprawidłowości. Po sprawdzeniu danych zawartych na dokumencie wejściowym z danymi zapisanymi w pamięci serwera obsługa kasy reklamacyjnej będzie mieć możliwość podjęcia decyzji o wpuszczeniu Klienta/Kibica do obiektu poprzez wydanie biletu zastępczego lub niewpuszczeniu Klienta/Kibica do obiektu. System nie wpuści do obiektu Klienta/Kibica z zakazem stadionowym lub klubowym, a także Klienta/Kibica posługującego się fałszywym dokumentem wejściowym lub dokumentem, który już raz został użyty.

System będzie umożliwiać pełną identyfikację Klientów/Kibiców na etapie sprzedaży dokumentu wejściowego, składania wniosku o elektroniczną kartę klienta/kibica, kontroli dokumentów wejściowych w punktach kontrolnych, a także w dowolnym momencie trwania imprezy masowej. Szczegółowa koncepcja procesu identyfikacji osób wchodzących została opisana w dalszej części niniejszej dokumentacji.

System będzie umożliwiać współpracę z terminalami płatniczymi do realizacji płatności bezgotówkowych bankowymi kartami płatniczymi poprzez automatyczne przekazywanie szczegółów transakcji do terminala płatniczego bez konieczności osobnego wprowadzania szczegółów transakcji do terminala oraz przyjmowanie informacji zwrotnej z terminala o dokonanej transakcji.

System będzie umożliwiać kompleksową obsługę Klientów/Kibiców poprzez sklep www w zakresie rejestracji profilu, złożenia i opłacenia wniosku o wydanie karty klienta/kibica, zakupu dokumentów wejściowych, produktów i usług oferowanych przez Inwestora, oraz uzyskania wszechstronnych informacji dotyczących imprez organizowanych na obiektach.

System będzie umożliwiać nadawanie uprawnień Użytkownikom Oprogramowania poprzez ograniczenie dostępności do jego zasobów i funkcji.

Oprogramowanie będzie zapewniać szczelność Systemu przed wtargnięciem do Bazy Danych przez osoby nieupoważnione. Ponadto Oprogramowanie Systemu będzie

umożliwiać przechowywanie wszystkich informacji w Bazie Danych Systemu, będzie zbierać informacje o wszystkich transakcjach sprzedaży, umożliwiać tworzenie raportów i sprawozdań z funkcjonowania obiektu i Systemu, a także sprawdzać i raportować poprawność funkcjonowania poszczególnych punktów kontrolnych i urządzeń końcowych.

W Systemie będzie istnieć możliwość wyłączenia systemu komputerowego (platformy serwerowej w całości lub częściowo) w trakcie wpuszczania osób na obiekty bez zatrzymywania ruchu osobowego przez punkty kontrolne i bez utraty informacji zbieranych w trakcie wpuszczania osób na halę lub stadion. System będzie mieć możliwość pracy w trybie off-line poprzez sprawdzarki biletowe posiadające pamięć wewnętrzną na 25 tys. rekordów uprawnionych dokumentów wejściowych oraz danych osobowych uprawnionych do wejścia osób, a także 50tys. rekordów zapisanych transakcji, oraz poprzez nieprzerwaną pracę Systemu z wykorzystaniem zasilania gwarantowanego obiektu. System będzie umożliwiać dalsze wpuszczanie osób do obiektu bez zatrzymywania pracy kołowrotów i punktów kontrolnych oraz utraty informacji.

9.7. Wymagania systemowe i platforma serwerowa

9.7.1. Platforma serwerowa

System będzie pracować w oparciu o platformę serwerową i wyodrębnionych na niej funkcjonalnych serwerach wirtualnych.

Platforma serwerowa będzie się składać z jednej fizycznej maszyny.

Serwer będzie charakteryzował się następującymi cechami i parametrami technicznymi:

1) Obudowa - Obudowa o wysokości max 2U do instalacji w standardowej szafie rack 19" z kompletem kabli i przewodów połączeniowych do podłączenia zestawu.

2) Wewnętrzna pamięć masowa - Zainstalowane 4 sztuki dysków Hot Plug SSD 240GB każdy.

3) Kontroler pamięci masowej - Zainstalowany wewnętrzny sprzętowy kontroler pamięci masowej, posiadający 1GB nieulotnej pamięci cache, umożliwiającą konfigurację poziomów RAID : 0, 1, 5, 6, 10, 50, 60 na zainstalowanych w/w dyskach.

4) Procesor - procesor 10 rdzeniowy(20 wątków) o taktowaniu 2.3 GHz.

5) Interfejsy sieciowe - 4 porty RJ-45 1Gbit.

6) Pamięć RAM - Zainstalowane 64GB pamięci DDR4.

7) Zasilanie - 2 zasilacze HotPlug z możliwością pracy w redundancji.

8) Gwarancja - Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, zgłaszanie awarii w trybie 24x7x365.

9) Wbudowane porty - 1x port USB na panelu przednim oraz 1x port USB na panelu tylnym.

10) Karta zarządzająca - Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiającą:

a) zdalny dostęp do graficznego interfejsu Web karty zarządzającej

- b) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,)
- c) szyfrowane połączenie oraz autentykację i autoryzację użytkownika
- d) wirtualną konsolę z dostępem do myszy, klawiatury
- e) wsparcie dla SNMP; IPMI2.0, SSH

Na serwerze będzie zastosowana macierz typu RAID 10 co zapewni zwiększoną szybkość operacji zapisu i odczytu wymaganą do obsługi bazy danych SQL. Rozwiązanie to zapewni zwiększoną odporność Systemu na uszkodzenie dysku.

W celu zwiększenia bezpieczeństwa przechowywania gromadzonych danych będzie zastosowana zewnętrzna macierz. Na zewnętrznej macierzy dyskowej także będzie zastosowana Macierz typu RAID 10. Będą na niej przechowywane kopie Systemu umożliwiające szybkie odtworzenie Systemu w przypadku zniszczenia platformy serwerowej np. pożaru serwerowni.

Parametry techniczne macierzy zewnętrznej

- a) procesor: dwurdzeniowy o częstotliwości zegara 2,41 GHz Pamięć RAM: 1 GB DDR3
- b) Ilość dysków: 4 x 3.5" WD Red
- c) pojemność dysków: 1TB (każdy dysk)
- d) interfejsy sieciowe: 2 x Gigabit RJ-45 Ethernet
- e) dostępne tryby RAID: RAID 0, 1, 5, 6, 10
- f) wersja rack
- g) obsługa protokołów: NFS, FTP
- h) dostęp i administracja poprzez HTTPS (SSL)

Zasoby dyskowe serwera będzie umożliwiać przechowywanie danych z imprez masowych przez okres min. 60 dni.

System będzie pracować na serwerze relacyjnej Bazy Danych MySQL.

Baza Danych Systemu pomieści informacje o 100 tys. Klientów/Kibiców.

Specyfikacja funkcjonalna serwerów wirtualnych została opisana w dalszej części projektu.

9.7.2. Serwery funkcjonalne Systemu

Na platformie serwerowej Systemu będą wyodrębnione następujące serwery funkcjonalne:

Serwer bazodanowy – będzie przechowywać całość informacji o bazie danych Klientów/Kibiców, imprezach, cennikach, widowni, udostępniać informacje z bazy dla serwera sklepu www, aplikacji kasjerskiej i serwera kontroli, umożliwiać tworzenie kopii zapasowych i replikację bazy danych oraz cykliczne archiwizować dane.

Serwer aplikacyjny – będzie udostępniać aplikacje dla kasjerów i pośredników w Punktach Sprzedaży, umożliwiać gromadzenie i budowanie bazy danych Klientów/Kibiców w Punktach Sprzedaży, obsługiwać proces rezerwacji i sprzedaży

Dokumentów Wejściowych, produktów, umożliwiać składanie elektronicznych wniosków o Karty Klienta/Kibica w Punktach (wstępna rezerwacja miejsc, zwalnianie biletów, bez potwierdzenia wpłaty, itp.) a także sprawdzać dostępność obiektów.

Serwer sklepu www – będzie umożliwiać gromadzenie i budowanie bazy danych Klientów/Kibiców poprzez sklep www, kontrolować i uzupełniać informacje w bazie internetowej (wystawianie imprez, do sprzedaży w portalu www), obsługiwać proces rezerwacji i sprzedaży biletów, przez Internet oraz składanie elektronicznych wniosków o Karty Klienta/Kibica (wstępna rezerwacja miejsc, dla klientów internetowych, zwalnianie biletów, bez potwierdzenia wpłaty, zakup dokumentu wejściowego z płatnością definitywną, itp.).

Serwer kontroli biletów– będzie przechowywać informację o bazie danych Klientów/Kibiców uprawnionych do wejścia, umożliwiać komunikację ze sprawdzarkami biletowymi, umożliwiać trwałe wiązanie wizerunku Klienta/Kibica w momencie czytania Dokumentu Wejściowego z numerem tego Dokumentu Wejściowego i danymi osobowymi Klienta/Kibica. Serwer będzie na bieżąco odczytywać poziom zapęnlienia obiektu i poszczególnych stref, przechowywać informację o wykrytych nieprawidłowościach w rozpoznawanych biletach w Punktach Kontroli, ułatwiać rozpatrywanie reklamacji.

Serwer monitoringu pracy Systemu – będzie umożliwiać monitorowanie pracy poszczególnych elementów Systemu, zgodnie z opisem znajdującym się w akapicie „Monitoring poprawnej pracy Systemu”.

9.7.3. Monitoring poprawnej pracy Systemu

Na platformie serwerowej zostanie wydzielony jeden zwirtualizowany serwer pełniący funkcję monitorującą poszczególne elementy Systemu (oprogramowanie Zabbix). Uszkodzenie jednego z elementów Systemu zostanie zarejestrowane oraz zasygnalizowane Administratorowi Systemu poprzez aktywne kanały powiadomień.

Podstawowe funkcjonalności systemu monitoringu:

- a) wykrywanie awarii i wysyłanie powiadomień za pomocą email lub SMS, wyświetlanie informacji na graficznym panelu informacyjnym,
- b) możliwość tworzenia mapy sieci,
- c) komunikacja z urządzeniami z wykorzystaniem protokołu SNMP,
- d) możliwość tworzenie scenariuszy testowych,
- e) pełne raportowanie zdarzeń,
- f) raportowanie zarówno awarii, jak i przekroczonych stanów krytycznych np. ilość wolnego miejsca na dysku poniżej wymaganego progu 10%,
- g) graficzne przedstawianie zebranych danych,
- h) automatyczne wykonywanie działań naprawczych w sytuacjach awaryjnych np. restart usługi,

- i) możliwość podłączenia się do systemu monitoringu z dowolnego miejsca za pomocą przeglądarki internetowej,
- j) równoległa praca wielu użytkowników,
- k) gromadzenie danych w relacyjnej bazie danych SQL,
- l) możliwość wykonywania poleceń przez serwer na urządzeniach podłączonych do systemu monitoringu.

9.7.4. Firewall - Zabezpieczenie serwera WWW

W celu podniesienia bezpieczeństwa systemu oraz jego zabezpieczenia przed nieautoryzowanym dostępem do serwera www i aplikacji kasjerskiej zostanie zainstalowany i skonfigurowany firewall z routerem spełniający następujące minimalne parametry techniczne:

- a) WYPOSAŻONY W SYSTEM IDS i IPS
- b) WYDAJNOŚĆ:
 - ☐ przepustowość firewall z włączonym IPS – przynajmniej 400 Mbps
 - ☐ przepustowość VPN (AES) – przynajmniej 100 Mbps
 - ☐ równoczesne połączenia – przynajmniej 75 000
 - ☐ liczba nowych sesji/sekundę – przynajmniej 5000
 - ☐ nielimitowana liczba użytkowników
- c) OCHRONA:
 - ☐ wykrywanie i kontrola aplikacji
 - ☐ kontrola ruchu aplikacji
 - ☐ analiza ruchu SSL
 - ☐ liczba reguł filtrowania – przynajmniej 1000
- d) FILTROWANIE TREŚCI:
 - ☐ filtrowanie URL (16 kategorii)
- e) UŻYTKOWNICY:
 - ☐ integracja z Active Directory
 - ☐ wewnętrzna i zewnętrzna baza LDAP
- f) INNE:
 - ☐ usługi QoS
 - ☐ routing dynamiczny
 - ☐ liczba tuneli SSL VPN – przynajmniej 20
 - ☐ Liczba obsługiwanych VLAN (802.1q) – przynajmniej 64
 - ☐ Ilość tuneli IPsec VPN – przynajmniej 50
 - ☐ Ilość tuneli PPTP – przynajmniej 48

Urządzenie będzie zapewniło bezpieczeństwo systemu informatycznego zgodnie z Rozporządzeniem MSWiA z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz.1024) oraz ustawy o ochronie danych osobowych.

9.7.5. Backup Systemu

System zostanie wyposażony w mechanizm archiwizacji umożliwiający jego

konfigurację w momencie instalacji Systemu wg wytycznych Inwestora ustalonych w czasie analizy przedwdrożeniowej oraz na podstawie Polityki Bezpieczeństwa Danych Osobowych Inwestora. Zastosowane rozwiązanie za pomocą oprogramowania Duplicity umożliwi wykonywanie pełnej kopii bazy danych wraz z całym Systemem w każdą sobotę oraz kopii przyrostowych codziennie w dni powszednie. Kopie wykonywane będą o godz. 1:00. Utworzona kopia będzie automatycznie zapisywana na serwerze. Rozwiązanie pozwoli również na wskazanie przez Inwestora dodatkowego, drugiego miejsca przechowywania danych zapasowych i ich automatyczne przekazywanie we wskazane miejsce. Takie działanie pozwoli na szybsze odtworzenie Systemu na nowym sprzęcie w przypadku całkowitego zniszczenia serwera (np. w sytuacji pożaru serwerowni). W momencie instalacji Systemu zdefiniuje się okres przechowywania codziennych backupów. Ich przechowywanie obejmuje co najmniej okres jednego miesiąca od ich wykonania. W przypadku wykonania przez obsługę Systemu krytycznej operacji, wymagającej przywrócenie kopii z dnia poprzedniego, czas potrzebny na jej odtworzenie wyniesie do kilku godzin w zależności od rozmiaru bazy.

9.7.6. Pozostałe wymagania systemowe

Aplikacje sklepu www posadowione na serwerze Systemu będą zawierać dane tylko i wyłącznie danego obiektu i imprez Inwestora. Właścicielem serwera z zainstalowanym serwisem sklepu www z biletami będzie Inwestor.

System będzie umożliwiać limitowany dostęp dla określonych Użytkowników. Inwestor wskaże osobne adresy internetowe dla aplikacji kasjerskich, aplikacji do rejestracji mediów i wydawania akredytacji oraz sklepów www pod którymi będzie skonfigurowany System.

Sklep www będzie współpracować z operatorem płatności internetowych np. PayU i umożliwiać płatność definitywną w sklepie www za zakupione produkty i Dokumenty Wejściowe.

Aplikacja/sklep www będzie pracować w trybie rezerwacji lub sprzedaży biletów i kartetów oraz składania elektronicznych wniosków o Kartę Klienta/Kibica. W sklepie www będzie możliwość utworzenia wersji językowych oraz rejestracji i zakupu Dokumentów Wejściowych i usług na obcojęzycznej wersji sklepu www dla obcokrajowców nie posiadających numeru PESEL, a chcących uczestniczyć w imprezie (w tym imprezie masowej podwyższonego ryzyka).

Sklep www umożliwi prezentowanie w sklepie www następujących dokumentów i informacji:

- a) regulaminu sklepu/sprzedaży przez www,
- b) regulaminu wydawania Kart Klienta/Kibica,
- c) regulaminu obiektu,
- d) kilku aktualności (zmienianych i aktualizowanych przez Administratora lub uprawnionego Użytkownika Systemu),
- e) widoku/planu obiektu z podziałem na strefy i sektory,
- f) mapki dojazdu do stadionu z zaznaczeniem między innymi parkingów, przystanków komunikacji miejskiej, sanitariatów, kas, depozytów i innych istotnych

elementów,

- g) FAQ-u,
- h) cenników i terminarzy imprez,
- i) podlinkowanych logotypów sponsorów lub partnerów,
- j) rotujących banerów centralnych z możliwością podlinkowania każdego baneru z osobna i określenia częstotliwości rotacji banerów.

W sklepie www będzie istnieć możliwość zbierania minimum następujących oświadczeń woli – zgód na:

- a) przetwarzanie obowiązkowych danych osobowych wynikających z ustawy o BIM i ustawy o świadczeniu usług drogą elektroniczną,
- b) przetwarzanie nieobowiązkowych danych osobowych,
- c) zapoznanie się i akceptację regulaminu sklepu www.

Na serwerach i urządzeniach Systemu będzie zainstalowane niezbędne Oprogramowanie Narzędziowe i Systemowe umożliwiające poprawną pracę Systemu. Symetryczne łącze internetowe o przepustowości min. 10Mbps/10Mbps na obiekcie, z możliwością rozszerzania łącza na okres najbardziej intensywnej sprzedaży, umożliwiające pracę sklepu www zapewni Inwestor. Wykonawca zagwarantuje poprawną pracę Systemu na dostarczonym przez Inwestora łączu o podanych parametrach.

Użytkowanie Systemu musi być realizowane zgodnie z wytycznymi Producenta Oprogramowania i urządzeń w zakresie jego poprawnej eksploatacji i konserwacji.

9.8. Moduł Budowania i Zarządzania Bazą Klientów

9.8.1. Typy Klientów

System będzie umożliwiać obsługę następujących Typów Klientów:

a) Klient Indywidualny Anonimowy – kontakt jednorazowy, polegający na wykupieniu produktów lub usług Inwestora /Użytkownika w Punktach Sprzedaży, możliwość rejestracji w Systemie (założenie profilu w Punkcie Sprzedaży lub poprzez sklep www).

b) Klient Grupowy Anonimowy – kontakt jednorazowy, polegający na wykupieniu produktów lub usług Inwestora w Punktach sprzedaży dla większej liczby osób.

c) Klient Indywidualny – zarejestrowany w Systemie – Klient zarejestrowany w Systemie, w Punkcie Sprzedaży lub poprzez sklep www. Możliwość złożenia wniosku o wydanie Imiennej Karty Klienta/Kibica, możliwość zakupu Dokumentów Wejściowych poprzez sklep www i sprawdzania historii wykupionych produktów, możliwość sprawdzenia dostępnych promocji, cenników i dedykowanych dla danego Typu Klienta, możliwość otrzymywania faktur zarówno w Punktach Sprzedaży jak i poprzez sklep www.

d) Klient Grupowy/Firmowy – zarejestrowany w Systemie. Dla Klienta Firmowego/Grupowego będzie istnieć możliwość pobierania danych firmowych jak np. NIP, nazwa firmy oraz definiowania innych danych niż dla Klienta Indywidualnego koniecznych do zakupu biletów. W Systemie będzie możliwość sprzedaży wielu biletów dla Klienta Grupowego/Firmowego, oraz możliwość otrzymywania faktur.

e) Klient Techniczny – pracownik Inwestora, służb zaangażowanych w organizację i zabezpieczenie imprezy, a w szczególności służb medycznych, Ochrony i Policji, dla którego wydawana jest Karta Techniczna.

9.8.2. Zarządzanie bazą klientów

System będzie umożliwiać rejestrację, budowanie i zarządzanie bazą Klientów poprzez:

a) zakładanie profili Klientów Indywidualnych - w Punktach Sprzedaży jak i poprzez sklep www, Firmowych - w Punktach Sprzedaży, a także Klientów Technicznych z poziomu Administratora lub uprawnionego Użytkownika.

b) rejestrację Klientów, blokowanie w Systemie (profilu Klienta) okienek z obowiązkowymi Danymi Osobowymi po weryfikacji tych danych i tożsamości Klienta w Punkcie Sprzedaży (po weryfikacji tożsamości Klienta i zablokowaniu jego profilu w Systemie, System będzie uniemożliwiać edycję i zmianę tych danych poprzez sklep www).

c) szybkie i bezbłędne wprowadzanie danych oraz weryfikację tożsamości Klienta w Punktach Sprzedaży, wprowadzanie wizerunku Klienta za pomocą kamery internetowej.

d) weryfikacja tożsamości kibica za pomocą czytników poprzez skanowanie czcionki zawartej w strefie MRZ w dowodzie osobistym,

e) automatyczne wyszukiwanie zarejestrowanych Klientów za pomocą: czytnika kart RFID, czytnika OCR, imienia, nazwiska, numeru PESEL.

f) autoryzację Klienta w sklepie www za pomocą numeru PESEL i hasła, adresu e-mail i hasła albo za pomocą adresu e-mail lub numeru PESEL i hasła. W Systemie będą istnieć wszystkie trzy sposoby autoryzacji.

g) autoryzację Użytkownika w Systemie (kasjera, sprzedawcy w punkcie sprzedaży poza obiektem, itp.) poprzez wpisanie loginu i hasła.

h) aktywację i dezaktywację profili Klientów.

i) wprowadzanie zakazów stadionowych i klubowych do profilu Klienta wraz z terminem ich obowiązywania oraz możliwością podpięcia pliku (skanu konkretnego wyroku).

System umożliwia osobne definiowanie pól obowiązkowych i nieobowiązkowych w formularzu rejestracyjnym profilu Klienta.

System umożliwia gromadzenie danych wymaganych przez ustawę o BIM – imienia, nazwiska, numeru PESEL.

System umożliwia definiowanie pól nieobowiązkowych – np. z danymi marketingowymi, których wypełnienie przy rejestracji/zakładaniu profilu lub w okresie późniejszym jest zależne od Klienta i wyrażenia przez niego zgody na przetwarzanie danych marketingowych.

System umożliwia zbieranie i rejestrowanie zgody Klientów na przetwarzanie danych obowiązkowych (wymaganych przez ustawę o BIM) oraz danych nieobowiązkowych i marketingowych.

System będzie gromadzić informacje o wszystkich danych klientów, kartach oraz

dokonanych transakcjach sprzedaży, rezerwacji i stornowania. W zakresie zarządzania bazą klientów System umożliwi:

- a) realizację akcji mailingowych,
- b) stosowanie zniżek, upustów, rabatów, promocji dla wybranych grup klientów.

9.8.3. Karty Klienta/Kibica

System umożliwi wydawanie następujących Typów Kart Klienta/Kibica:

a) Karta Imienna – umożliwiająca pełną identyfikację Klienta/Kibica zgodnie z wymaganiami ustawy o BIM, zawierająca dane osobowe Klienta/Kibica (imię, nazwisko, numer PESEL oraz opcjonalnie, zdjęcie).

b) Karta Firmowa – karta z oznaczeniem Klienta Firmowego, dla którego jest wydana. System umożliwi wydawanie kilku Kart Firmowych dla jednego Klienta Firmowego.

c) Karta Techniczna – Karta wydawana dla pracowników Inwestora, Służb Ochrony, Policji, Służb Technicznych.

W przypadku Kart Imiennych System będzie umożliwiać składanie i opłacanie wniosków o wydanie Karty Klienta/Kibica zarówno w Punktach Sprzedaży, jak i przez sklep www.

System umożliwi zarządzanie bazą elektronicznych wniosków o wydanie Kart Klienta/Kibica, przede wszystkim poprzez:

- a) elektroniczne przyjmowanie wniosków o wyrobienie Karty Klienta/Kibica wraz z możliwością ich opłacenia zarówno przez witrynę www, jak i w Punktach Sprzedaży,
- b) potwierdzanie przyjęcia wniosku o wydanie Karty Klienta/Kibica w Systemie przez pracownika Inwestora /Użytkownika Końcowego,
- c) drukowania i wydawanie kart klienta/kibica,
- d) drukowanie i personalizowanie Kart Klienta/Kibica z Systemu dla wielu Klientów i złożonych wniosków jednocześnie, z tym przez sklep www,
- e) wybór wzoru graficznego Karty Kibica w momencie składania wniosku w Punkcie Sprzedaży jak też przez sklep www,
- f) wydawanie duplikatów Kart,
- g) blokowanie zagubionych lub skradzionych Kart Klienta/Kibica,
- h) możliwość określenia ważności Karty Klienta/Kibica przez określony czas od jej wydania lub do konkretnej daty zdefiniowanej w Systemie.

W momencie składania elektronicznego wniosku o wydanie Karty Klienta/Kibica System umożliwi wybór opcji dostawy Karty:

- a) odbiór osobisty,
- b) wysyłka pocztą,
- c) wysyłka kurierem

oraz przypisze odpowiednią, zdefiniowaną w systemie cenę dostawy w zależności od wybranego sposobu dostawy.

Dla Kart Firmowych i Kart Technicznych wydawanie Kart będzie odbywać się w stacjonarnych Punktach Sprzedaży bez konieczności składania elektronicznego wniosku

Karta Klienta/Kibica w zależności od Typu Karty będzie pełnić funkcję:

- a) dokumentu identyfikacyjnego (dot. Kart Imiennych i Kart Technicznych),
- b) nośnika uprawnień do wejścia na Stadion (w formie elektronicznego biletu, karnetu, abonamentu, uprawnienia technicznego).

Funkcję Kart Klienta/Kibica będą pełnić karty z chipem RFID w standardzie MIFARE.

9.8.4. Aplikacja Rejestracji Mediów i Wydawania Akredytacji

System będzie umożliwiać składanie wniosków przez media o przyznanie akredytacji będącej równocześnie dokumentem wejściowym. Aplikacja do składania wniosków dla mediów będzie znajdować się na osobnym adresie internetowym wskazanym przez Inwestora (innym niż sklep www dla Klientów/Kibiców).

Każdy dziennikarz chcąc złożyć wniosek o wydanie akredytacji (będącej jednocześnie dokumentem wejściowym do obiektu) będzie musiał swój profil klienta indywidualnego w systemie. Założenie profilu nastąpi poprzez wypełnienie formularza rejestracyjnego oraz aktywację linku wysłanego z systemu na adres mailowy wskazany w procesie rejestracji. Założenie i aktywacja profilu dla dziennikarza automatycznie utworzy i aktywuje profil w bazie danych Klientów i umożliwi korzystanie z systemu (jako Klient/Kibic) poprzez ten sam login i hasło zarówno w sklepie www, jak i w aplikacji do rejestracji mediów i wydawania akredytacji. Autoryzacja osoby w aplikacji do rejestracji mediów będzie odbywać się na takiej samej zasadzie, jak w sklepie www czyli za pomocą numeru PESEL i hasła, adresu e-mail i hasła albo za pomocą adresu e-mail lub numeru PESEL i hasła. W systemie będą istniały wszystkie trzy sposoby autoryzacji. Zmiana sposobu autoryzacji będzie możliwa do wykonania na etapie eksploatacji.

W procesie rejestracji/zakładania profilu aplikacja umożliwi wprowadzenie następujących danych:

- a) imienia (osoby ubiegającej się)
- b) nazwiska (osoby ubiegającej się)
- c) daty urodzenia
- d) numeru PESEL (lub rodzaju i numeru dokumentu tożsamości dla obcokrajowców)
- e) adresu e-mail (osoby ubiegającej się)
- f) numeru telefonu (osoby ubiegającej się)
- g) uwag/wiadomości

Aplikacja umożliwi również przesłanie (dołączenie pliku) ze zdjęciem osoby rejestrującej się.

Aplikacja umożliwi również rejestrację i składanie wniosków o wydanie akredytacji dla obcokrajowców (osób nie posiadających numeru PESEL) i w przypadku wybrania narodowości innej niż Polska system będzie wymagać podania płci, rodzaju i numeru dokumentu tożsamości oraz daty urodzenia, zamiast numeru PESEL.

Przy zakładaniu profilu dla mediów system będzie weryfikował czy dana osoba nie

posiada zakazu stadionowego lub klubowego.

Aplikacja umożliwi również sprawdzanie posiadanych zakazów stadionowych i klubowych na etapie składania wniosków o przyznanie akredytacji oraz uniemożliwi złożenie wniosku o akredytację osobie posiadającej zakaz stadionowy lub klubowy.

Aplikacja umożliwi zbieranie i rejestrowanie zgody Klientów na przetwarzanie danych obowiązkowych (wymaganych przez ustawę o BIM) oraz danych nieobowiązkowych i marketingowych.

Po założeniu profilu i zalogowaniu się na swoje konto System będzie umożliwiał złożenie wniosku o akredytację dla mediów. System umożliwi zdefiniowanie i wybranie przez osobę składającą wniosek następujących informacji:

a) Rodzaju akredytacji: stałej (na daną rundę rozgrywkową) lub jednorazowej (na dany mecz). W przypadku akredytacji jednorazowej będzie istniał wybór imprezy na którą przyznawana będzie akredytacja.

b) Typu akredytacji z rozwijanej listy dostępnych typów, generowanej na podstawie kalendarza imprez dostępnego w systemie, według stref dostępu np. foto z dostępem na murawę, media klub z dostępem na murawę i innych zdefiniowanych przez Zamawiającego na etapie analizy przedwdrożeniowej.

Przy składaniu wniosku o akredytację system umożliwi przypisanie do danego wniosku danych redakcji, którą będzie reprezentować osoba składająca wniosek. Aplikacja umożliwi wprowadzenie następujących danych:

- a) imienia (redaktora naczelnego)
- b) nazwiska (redaktora naczelnego)
- c) nazwy redakcji
- d) adresu redakcji (kod pocztowy, miasto, ulica)
- e) adresu e-mail redakcji
- f) adresu strony www redakcji
- g) numeru telefonu kontaktowego redakcji

Administrator lub uprawniony Użytkownik będzie miał możliwość:

- a) przeglądania w systemie złożonych wniosków o akredytację
- b) zatwierdzania złożonego wniosku
- c) drukowania akredytacji/dokumentów wejściowych z Systemu.

Aplikacja umożliwi drukowanie:

a. akredytacji stałych w postaci Kart Technicznych (kart RFID) według zdefiniowanego przez Zamawiającego layoutu oraz zdefiniowanych przez Zamawiającego na etapie analizy przedwdrożeniowej danych nadrukowywanych na karcie (minimum wymaganych danych to: wskazanie rundy na którą przyznana będzie akredytacja, nazwy reprezentowanej redakcji, imienia, nazwiska oraz wizerunku osoby).

b. akredytacji jednorazowych w postaci papierowej z kodem kreskowym 1D lub 2D według zdefiniowanego layoutu oraz zdefiniowanych danych nadrukowywanych na akredytacji (minimum wymaganych danych to: nazwa imprezy, na którą będzie przyznana akredytacja, imię, nazwisko wizerunek osoby).

Aplikacja automatycznie będzie wysyłała powiadomienia w formie mailowej na adresy

wskazane w systemie (zarówno adres mailowy osoby ubiegającej się, jak i adres mailowy redakcji) o przyznaniu lub odmowie przyznania akredytacji.

Aplikacja umożliwi wygenerowanie listy przyznanych akredytacji stałych i jednorazowych na daną imprezę oraz eksport listy w formacie txt lub csv.

Przedstawiciele mediów, którzy uzyskają akredytację będą mieli możliwość jej odebrania w Punkcie Obsługi Mediów, gdzie po okazaniu dokumentu tożsamości i identyfikacji osoby, która złożyła wniosek i dla której została przyznana akredytacja będzie można w systemie zablokować profil Klienta/Kibica z obowiązkowymi danymi osobowymi, tak aby osoba z odebraną akredytacją nie mogła zmienić na stronie internetowej, w aplikacji do składania wniosków dla mediów swoich danych obowiązkowych. Potwierdzenie i zablokowanie profilu danej osoby w aplikacji umożliwi korzystanie przez nią ze wszystkich funkcjonalności dostępnych w Systemie dla osób z zablokowanym profilem również w sklepie www.

Każdy Użytkownik/Klient po zalogowaniu się do swojego profilu będzie miał możliwość podglądu swoich danych osobowych oraz złożonych wniosków o akredytację i przyznanych akredytacji.

9.8.5. Wydawanie identyfikatorów wewnętrznych

Aplikacja do wydawania akredytacji wewnętrznych (identyfikatorów) służy do wydawania akredytacji jedynie z poziomu aplikacji kasjerskiej (uprawnionego użytkownika/administratora). Bazuje w Systemie na profilu klienta firmowego, dla którego nie wymagane jest podawanie numeru PESEL.

Uprawniony użytkownik (kasjer/administrator) z poziomu aplikacji kasjerskiej założy profil klienta firmowego i przypisze do go puli klientów AKREDYTACJE. Uzyska wtedy możliwość uzupełnienia dodatkowych pól dedykowanych dla tej puli klientów firmowych: FIRMA, FUNKCJA oraz wybrania dostępnych dla danego klienta stref dostępu, zgodnie z poniższą listą (przesłaną w regulaminie akredytacji)

- AAA – wstęp do wszystkich stref;
- AAA* – wstęp do wszystkich stref z możliwością wprowadzania osób nie posiadających uprawnień do wejścia do danej strefy;
- 0 – strefa szatni;
- 1 – strefa techniczna boiska;
- 2 – murawa boiska;
- 3 – trybuna prasowa;
- 4 – konferencja prasowa;
- 5 - strefa biurowa;
- 6 – strefa biznes (Klub Biznesowy, łoże);
- 7 – możliwość przejścia między trybunami;
- 8 – wejście na sektor gości i do strefy przyjęcia kibiców gości;
- 9 – stanowisko dowodzenia.

System umożliwi zaznaczenie kilku stref dostępu dla danego klienta i numery przypisane do danej strefy drukowane będą na blankiecie akredytacji. Strefy dostępu nie będą w żaden sposób powiązane z systemem kontroli wejścia i punktami kontrolnymi i

będą stanowić tylko drukowaną informację na blankiecie akredytacji. Akredytacja będzie mogła być wydawana na pojedynczą imprezę lub całą rundę i zawierać kod kreskowy przypisany do sektora wirtualnego. Kod kreskowy uprawnii do wejścia przez zdefiniowany punkt kontrolny. System umożliwi stworzenie i wygenerowanie statystyki - dla kogo została wydana akredytacja na daną rundę lub imprezę i przez jakiego kasjera/użytkownika. W statystyce nie będzie podglądu stref (informacji drukowanych na blankiecie akredytacji), na jakie została wydana dana akredytacja.

9.9. Moduł Sprzedaży Dokumentów Wejściowych

9.9.1. Ogólne wymagania i ustawienia konfiguracyjne Modułu

Moduł będzie umożliwiać sprzedaż Dokumentów Wejściowych na różnego typu imprezy masowe odbywające się na hali lub stadionie – imprezy sportowe, w tym podlegające ustawie o BIM, koncerty, eventy.

Moduł umożliwi również sprzedaż dodatkowych produktów i usług - np. gadżetów kupowanych do biletu (szalików, czapek kibica, etc.).

System będzie pracować w formie aplikacji serwerowej (witryna internetowa), obsługiwanej poprzez przeglądarki internetowe zainstalowane w Punktach Sprzedaży.

Moduł Sprzedaży Dokumentów Wejściowych będzie umożliwiać:

- a) definiowanie innego rozkładu trybun, sektorów i miejsc w sektorach dla każdej imprezy oddzielnie,
- b) tworzenie sektorów wirtualnych,
- c) tworzenie sektorów nienumerowanych (np. na płycie boiska) z określoną pojemnością,
- d) definiowanie kluczy wejścia dla każdego sektora/strefy (który sektor/trybuna jest uprawniona do wejścia przez dany kołokrąg), przy czym będzie istnieć możliwość wpuszczenia połowy sektora przez jedno wejście a połowy przez inne,
- e) blokowanie stałe lub czasowe poszczególnych miejsc do sprzedaży na daną imprezę i dla poszczególnych sprzedawców (kontyngentów),
- f) prostą i szybką zmianę sprzedawcy/kasjera na danym stanowisku kasowym,
- g) utworzenie 3 wersji językowych sklepu www,
- h) definiowanie przez Administratora Systemu różnych typów biletów dla danej imprezy/obiektu oraz sprzedaż wielu typów biletów dla danej imprezy/obiektu jednocześnie,
- i) definiowanie ilości biletów do rezerwacji/sprzedaży dla 1 użytkownika w jednej transakcji oraz sumarycznie dla 1 imprezy,
- j) wizualizację graficzną obiektu, trybun i sektorów tak na stanowiskach kasowych, jak również w sklepie WWW oraz na wydrukowanych biletach formatu A4 (print@home),
- k) wybór miejsca siedzącego na obiekcie z uwzględnieniem sektora, rzędu i miejsca na podstawie graficznej interaktywnej mapy obiektu, trybuny, sektora i poszczególnych miejsc,
- l) definiowanie atrakcyjności miejsc w sektorze oraz atrakcyjności sektorów przez Administratora bez udziału Wykonawcy w celu automatycznego wskazywania miejsca dla kibica przez komputer zarówno w aplikacji kasjerskiej jak i sklepie www,

- m) dowolne definiowanie i konfigurowanie cenników dla wybranych Dokumentów Wejściowych, produktów, usług oraz grup Klientów,
- n) prostą modyfikację cenników biletów zarówno co do wartości poszczególnych kategorii cenowych, jak również co do liczby tych kategorii w zależności np. od trybuny, sektora, miejsca, przysługującej zniżki,
- o) różnicowanie cenników w zależności od kanału dystrybucji np. inny cennik w Punkcie Sprzedaży, a inny w sklepie internetowym,
- p) stosowanie wielu cenników i poziomów cenowych jednocześnie,
- q) definiowanie rabatów i narzutów,
- r) automatyczną zmianę cennika lub poziomu cenowego dla określonych typów Kart, Klientów,
- s) definiowanie opłat manipulacyjnych za zakup Dokumentu Wejściowego przez sklep www, w postaci kwotowej (dla danej ceny lub przedziału cen), procentowej oraz mieszanej (kwotowo-procentowej). System będzie umożliwiał przełączenie danej formy opłaty manipulacyjnej przez Administratora Systemu bez udziału Wykonawcy.
- t) obsługę „profilowanych” klientów z tzw. własnym zestawem cen, rabatów,
- u) konfigurowanie kalendarza imprez (jednoczesną sprzedaż biletów na wiele imprez, w tym również karnetów). Możliwość konfigurowania różnych rodzajów karnetów wzajemnie się przenikających – na imprezy całego sezonu, na wszystkie imprezy odbywające się danego dnia, na imprezy z udziałem konkretnej drużyny itp.,
- v) wymuszanie autoryzacji wybranych operacji dla zdefiniowanych kasjerów przez inną osobę poprzez automatyczną autoryzację polegającą na czytaniu karty MIFARE osoby autoryzującej (np. autoryzacja storna, ponownego wydruku, zwrotu biletu).

Moduł będzie uniemożliwiać sprzedaż Dokumentów Wejściowych na imprezy masowe osobom posiadającym zakazy stadionowe i klubowe.

W profilu Klienta będzie możliwość podpięcia pliku z wyrokiem/nałożonym zakazem stadionowym lub klubowym. Będzie również możliwość wprowadzenia do Systemu zakresu obowiązywania zakazu (od kiedy, do kiedy), informacji przez kogo został nałożony oraz dodatkowych uwag i komentarzy.

9.9.2. Rodzaje i typy Dokumentów Wejściowych

System będzie umożliwiać stosowanie następujących rodzajów Dokumentów Wejściowych na halę i stadion:

- a) biletów papierowych i plastikowych z kodem kreskowym 1D lub 2D (kod kreskowy na bilecie jako unikatowy numer, jednoznacznie identyfikujący dokonaną transakcję (kupujący, data sprzedaży, dane sprzedawcy, itp.) w bazie danych Systemu),
- b) biletów papierowych do samodzielnego wydruku w domu print@home (jako rezerwacja/lub opłacony Voucher uprawniający do odbioru biletu wstępu w Punktach Kasowych po zweryfikowaniu tożsamości Klienta/Kibica lub jako właściwy bilet wstępu – bilet print@home wydrukowany samodzielnie na dowolnej drukarce laserowej lub atramentowej w przypadku biletów na imprezy nie objęte ustawą o BIM lub w przypadku posiadania przez Klienta/Kibica zweryfikowanego profilu z potwierdzoną tożsamością),

c) biletów papierowych i kart plastikowych z chipem bezstykowym RFID (standard MIFARE ISO 14443A - unikalny kod nadawany w fazie produkcji pozwalający na zidentyfikowanie Klienta/Kibica i odczyt odpowiednich informacji z Bazy Danych Systemu).

d) Wirtualnych biletów wyświetlanych na urządzeniach mobilnych na podstawie odczytu QR Codu.

e) Biletów elektronicznych – których nośnikiem jest dowód osobisty (odczyt czcionki ze strefy MRZ)

System będzie umożliwiać sprzedaż następujących typów Dokumentów Wejściowych:

- a) pojedynczych i grupowych,
- b) normalnych i ulgowych,
- c) jednorazowych i karnetowych,
- d) VIP-owskich, specjalnych, zaproszeń i administracyjnych Dokumentów Wejściowych,
- e) rodzinnych, pakietowych w promocyjnej cenie np. 2+1, 2+2, 2+3 - w zależności od liczby dzieci i dorosłych w bilecie pakietowym,
- f) z przypisanym opiekunem do osoby niepełnoletniej na etapie zakupu biletu zgodnie z wymaganiami ustawy o BIM (System będzie umożliwiać zdefiniowanie dla jakiej grupy osób – w jakim wieku będzie wymagane przypisanie opiekuna wraz z rozgraniczeniem czy opiekun też musi/nie musi zakupić bilet - czy tylko będzie przypisany do osoby nieletniej w procesie zakupu danego biletu w celu wypełnienia zapisów ustawy o bezpieczeństwie imprez masowych),
- g) anonimowych i spersonalizowanych wraz z wizerunkiem klienta.

Przewiduje się dwa formaty dokumentów generowanych przez System:

a) Pierwszy rodzaj to właściwy Dokument Wejściowy opatrzony odpowiednim kodem kreskowym, zawierający chip RFID lub strefę MRZ umożliwiającą bezpośrednie otwarcie kołowrotu wejściowego na obiekt. W tym przypadku nie będzie konieczna wizyta klienta w kasie obiektu i może on być bezpośrednio skierowany do bram wejściowych,

b) Druga forma to Rezerwacja/Voucher wyposażony w identyfikator pozwalający na automatyczne wydanie właściwego biletu w punkcie sprzedaży obiektu po sczytaniu Vouchera przez Sprzedawcę, uzupełnieniu danych osobowych i/lub zweryfikowaniu tożsamości osoby wchodzącej oraz zablokowaniu profilu Klienta (okienek z obowiązkowymi danymi osobowymi). Będzie istnieć również możliwość ręcznego wpisania numeru Vouchera do Systemu i automatyczne wydanie właściwego biletu wstępu. System uniemożliwi ponowną wymianę Vouchera na bilet (uniemożliwienie wymiany skopiowanych Voucherów).

Końcowa forma graficzna i wzór Dokumentu Wejściowego oraz wymagane do umieszczenia na nim dane o imprezie i kupującym będą podlegać zatwierdzeniu przez Administratora – jednakże w przypadku imprez masowych podwyższonego ryzyka

muszą odpowiadać aktualnym zapisom ustawy o BIM. Będzie istnieć możliwość umieszczania na dokumencie wejściowym informacji marketingowych i dodatkowych wskazanych przez Administratora, jak np. wyciąg z regulaminu obiektu.

9.9.3. Szczegółowe funkcjonalności Modułu

Moduł sprzedaży Dokumentów Wejściowych będzie umożliwiać:

a) jednoczesną sprzedaż wszystkich rodzajów, typów i form Dokumentów Wejściowych opisanych w akapicie rodzaje i typy Dokumentów Wejściowych,

b) sprzedaż Dokumentów Wejściowych wg różnych scenariuszy dostosowanych do rodzaju imprez masowych i odpowiedniej aranżacji trybun i widowni, (odpowiednie do aranżacji rozplanowanie widowni z podziałem na sektory i numeracją poszczególnych miejsc w zależności od charakteru imprezy powinno zostać udostępnione Wykonawcy w postaci plików wsadowych (graficznych) dostawcy Systemu przez Administratora obiektu),

c) sprzedaż biletów/Dokumentów Wejściowych na dowolną ilość imprez masowych jednocześnie,

d) sprzedaż biletów w dowolnym czasie, na dowolną imprezę zdefiniowaną przez Administratora w Systemie,

e) sprzedaż w czasie rzeczywistym, z jednoczesnym dostępem do wszystkich wolnych miejsc przez wszystkich Sprzedawców,

f) opcjonalnie „sprzedaż szybką” w Punktach Sprzedaży, gdzie komputer wybiera automatycznie miejsce według zdefiniowanego przez Administratora schematu atrakcyjności miejsc,

g) sprzedaż innych produktów i usług (np. gadżetów kibica),

h) automatyczne przenoszenie rezerwacji miejsc karnetowych z poprzedniego sezonu,

i) tworzenie harmonogramów sprzedaży karnetów w podziale na zdefiniowane okresy:

☐ okres I - z prolongatą dla osób posiadających karnet w poprzednim/ej sezonie/rundzie na to samo miejsce (każda osoba, posiadająca karnet w poprzedniej rundzie ma założoną rezerwację miejsca z poprzedniej rundy i tylko na to miejsce może kupić karnet na kolejną rundę),

☐ okres II - z prolongatą dla osób posiadających karnet w poprzednim/ej sezonie/rundzie z przesiadkami na inne miejsce (każda osoba posiadająca karnet w poprzedniej rundzie ma założoną rezerwację miejsca z poprzedniej rundy, może kupić karnet na kolejną rundę na to samo miejsce lub z tego miejsca zrezygnować i wybrać inne),

☐ okres III - sprzedaż otwarta dla wszystkich kupujących na pozostałe wolne miejsca.

j) zakup i wydruk w domu biletu przez Klienta/Kibica, zaopatrzonego w kod kreskowy i numer weryfikacyjny,

k) doładowanie biletu/uprawnień do wejścia przez sklep www na Kartę Klienta/Kibica,

l) rezerwację miejsca/miejsc z określoną datą i/lub godziną automatycznego

wygaśnięcia rezerwacji (jeżeli do zdefiniowanego czasu rezerwacja nie zostanie opłacona, System będzie umożliwić ponowną sprzedaż zwolnionego miejsca),

m) definiowanie terminu wygaśnięcia rezerwacji w ilości dni lub do wyznaczonej daty i godziny,

n) wydłużenie okresu rezerwacji danego miejsca/miejsc przez Administratora lub uprawnionego Użytkownika/Sprzedawcę,

o) on-linową weryfikację zakazów klubowych/stadionowych na etapie sprzedaży biletu,

p) pełną identyfikację Klienta/Kibica na etapie sprzedaży biletu (poprzez wprowadzenie danych z dokumentu tożsamości, pobranie wizerunku Klienta/Kibica do Systemu i zablokowanie profilu Klienta/Kibica z obowiązkowymi danymi osobowymi),

q) realizację następujących form płatności:

- ☐ gotówka w Punktach Sprzedaży,
- ☐ karta bankomatowa lub karta kredytowa w Punktach Sprzedaży,
- ☐ płatności internetowe realizowane w sklepie www.

r) wystawianie faktur i duplikatów faktur z Systemu,

s) obsługę drukarek fiskalnych.

9.9.4. Kanały dystrybucji

System będzie zapewniać obsługę sprzedaży Dokumentów Wejściowych poprzez następujące kanały dystrybucji:

- a) Punkty Sprzedaży na obiekcie (Stanowiska Kasowe, Punkty Obsługi Klienta),
- b) Punkty Sprzedaży poza obiektem (Wyniesione Punkty Sprzedaży),
- c) zewnętrzne Punkty Sprzedaży,
- d) samoobsługowy sklep www.

9.9.5. Wyposażenie i funkcjonalność Punktów Sprzedaży

Na hali i stadionie sprzedaż Dokumentów Wejściowych prowadzona będzie na Stanowiskach Kasowych.

Na stadionie zlokalizowanych będzie 4 Stanowiska Kasowe (POS) w dwóch punktach kasowych. Każdy punkt kasowy będzie wyposażony w jedną dla wszystkich stanowisk drukarkę laserową do faktur i raportów. W jednym wskazanym punkcie kasowym zostanie zainstalowana drukarka sublimacyjna do kart plastikowych ENDURO 3E na potrzeby personalizacji kart klienta/kibica.

Wyposażenie każdego Stanowiska Kasowego:

- a) Zestaw komputerowy z procesorem Intel I3, 4GB RAM i HDD 500GB, system Windows, monitor dla obsługi oraz monitor dla klienta, mysz i klawiatura
- b) Stołowy czytnik kart RFID MIFARE SPORTDATA CKR USB
- c) Kamera internetowa np. Logitech C525.
- d) drukarka fiskalna z kopią elektroniczną np. Innova Profit EJ wraz z szufladą kasową,
- e) Drukarka termiczna do biletów np. BIXOLON SPL-D420,
- f) Czytnik kodów 1D, 2D oraz OCR – np. Xenon 1900.

Stanowisko Kasowe będzie umożliwiać: zbieranie i wprowadzanie do Systemu danych

osobowych Klientów/Kibiców i weryfikowanie tożsamości, pobieranie wizerunku kibica do Systemu za pomocą kamery internetowej, przyjmowanie elektronicznych wniosków o Imienną Kartę Klienta/Kibica i płatności za nie, drukowanie i wydawanie Imiennych Kart Klienta/Kibica, sprzedaż Dokumentów Wejściowych (biletów jednorazowych i karnetów), produktów i usług, automatyczną wymianę Voucherów na właściwe bilety wstępu, drukowanie biletów wstępu z rezerwacji internetowych, fiskalizację transakcji, stornowanie biletów, wystawianie i drukowanie faktur z Systemu, wydawanie Kart Firmowych, rozpatrywanie reklamacji z nieudanego wejścia kibica na obiekt – tylko na podstawie przeczytanego biletu (wyświetlenie wszystkich zdarzeń związanych z danym biletem i przejście do klatki wideo z momentu wejścia kibica na obiekt w czasie 1s.)

9.9.6. Raporty i statystyki Modułu

System umożliwia generowanie z Systemu minimum następujących raportów i statystyk:

- a) sporządzanie raportów sprzedaży dziennych i okresowych, pojedynczego kasjera, Punktu Sprzedaży, oddziału, kanału dystrybucji,
- b) bieżącą prezentację zapelnienia obiektu, stref, poszczególnych trybun i sektorów,
- c) generowanie raportów z każdej operacji sprzedaży,
- d) tworzenie raportów: dzienne zamknięcie kasjera, dzienne zamknięcie firmy,
- e) autozamykanie raportów kasjerskich o zdefiniowanej godzinie, w przypadku nie wykonania raportu przez kasjera,
- f) generowanie raportów kibiców z danymi osobowymi i wizerunkiem z danej imprezy w rozbiciu na poszczególne sektory,
- g) tworzenie statystyk: sprzedaż biletów na wybraną imprezę, sprzedaż biletów za dowolny okres, sprzedaż biletów z podziałem na firmy pośredniczące.

System umożliwia bieżący i archiwalny podgląd przez Administratora lub uprawnionego Użytkownika wszystkich transakcji wykonanych w Systemie. System umożliwia wyszukiwanie poszczególnych transakcji po nazwisku, numerze PESEL nabywcy/Klienta, numerze Karty Klienta, numerze transakcji, statusie transakcji, sprzedawcy, nazwie imprezy, kodzie kreskowym Dokumentu Wejściowego, okresie sprzedaży. Istnieje również możliwość sortowania transakcji według sprzedawcy, statusu transakcji, ilości biletów ogółem, metodzie płatności, sposobie dostawy, dacie transakcji, ID transakcji.

W Systemie będą prezentowane następujące statusy transakcji:

- a) zakończona,
- b) do zapłaty,
- c) oczekująca na płatność,
- d) wystornowana,
- e) anulowana.

9.10. Moduł Kontroli Biletów i Identyfikacji Kibiców

9.10.1. Budowa Modułu Kontroli Biletów i Identyfikacji Kibiców

Na Obiekcie będą zainstalowane urządzenia kontroli ruchu osobowego (kołowroty) ujęte w branży architektonicznej / budowlanej.

Każdy tor wejściowy urządzeń kontroli ruchu osobowego (bramy obrotowe wysokie i niskie oraz bramki uchylne ze sterowaniem elektromechanicznym) będą wyposażone w sprawdzarkę biletową zgodną z opisem, a bramy obrotowe wysokie dodatkowo w sygnalizator świetlny dla ochrony zgodny z opisem. Na każdej bramce uchylnej zostanie zainstalowana sprawdzarka biletowa wejściowa oraz wyjściowa służąca do obsługi chwilowych wyjść z obiektu.

Sprawdzarki biletowe będą weryfikować poprawność biletu, rozpoznawać bilety zniżkowe oraz sterować bramą obrotową i odbierać z niej sygnał zwrotny umożliwiający zaliczenie biletu na podstawie faktycznego przejścia osoby.

Sprawdzarki biletowe będą rozpoznawać wszystkie rodzaje i typy Dokumentów Wejściowych opisane w dokumentacji, w tym bilety zniżkowe oraz bilety osób poniżej 13-go roku życia prezentując tą informację:

a) dla kibica poprzez odpowiedni kolorowy znak i komunikat na wyświetlaczu LDC TFT sprawdzarki biletowej,

b) dla służb ochrony poprzez odpowiednią sygnalizację kolorystyczną na sygnalizatorze świetlnym w celu umożliwienia służbom ochrony sprawdzenia uprawnień do zniżek osoby wchodzącej lub obecności opiekuna osoby poniżej 13-go roku życia.

9.10.2. Funkcjonalność Modułu Kontroli Biletów i Identyfikacji kibiców

Moduł Kontroli Biletów i Identyfikacji Kibiców ze względu na swoje strategiczne znaczenie posiada wysoki stopień niezawodności. Umożliwia pracę Systemu w trybie off line oraz wpuszczanie kibiców bez przestojów w trybach awaryjnych. W przypadku awarii serwera zarządzającego lub w przypadku przerwanej komunikacji pomiędzy serwerem, a Punktami Kontrolnymi (w szczególności sprawdzarkami biletowymi) – sprawdzarki biletowe przejmują funkcjonalność Systemu umożliwiając pracę Punktu Kontrolnego (sprawdzarki biletowej) w trybie off line. Moduł Kontroli Biletów i Identyfikacji Kibiców umożliwia identyfikację osób wchodzących. Funkcjonalność ta będzie realizowana poprzez integrację Modułu Kontroli Biletów i Identyfikacji Kibiców z systemem CCTV.

Moduł Kontroli Biletów i Identyfikacji Kibiców będzie umożliwiać:

a) obsługę wszystkich rodzajów i typów Dokumentów Wejściowych jednocześnie dla danej imprezy wymienionych w akapicie rodzaje i typy Dokumentów Wejściowych niniejszego projektu,

b) określenie dostępu do wyznaczonych sektorów obiektu dla zdefiniowanych posiadaczy biletów,

c) skierowanie ruchu osobowego do dedykowanych wejść i wyjść (wybrane grupy biletów do wybranych grup bram obrotowych lub uchylnych) oraz całkowite blokowanie przejść przez nie (lub dla wybranych grup biletów),

d) weryfikację poprawności biletu w czasie nie dłuższym niż 1 sekunda,

- e) weryfikację aktualnych zakazów stadionowych i klubowych na etapie kontroli biletów (w tym również niewpuszczenie na obiekt osób, które otrzymały zakaz stadionowy lub klubowy już po nabyciu Dokumentu Wejściowego (biletu lub karnetu) na daną imprezę),
- f) integrację Modułu Kontroli Biletów i Identyfikacji Kibiców z systemem CCTV,
- g) eliminowanie ponownego użycia biletu oraz biletu fałszywego i nie należącego do puli danej imprezy,
- h) obsługę chwilowych wyjść z obiektu,
- i) chwilowe wyłączenie systemu bram obrotowych i bramek uchylnych bez wstrzymywania sprzedaży biletów,
- j) monitorowanie liczby osób będących na imprezie (w systemie on-line) oraz stopnia zapelnienia poszczególnych trybun,
- k) bieżącą prezentację zapelnienia obiektu w rozbiciu na poszczególne sektory, poszczególne wejścia oraz wszystkie wejścia razem,
- l) zapisanie w pamięci serwera daty i godziny sczytania Dokumentu Wejściowego i otwarcia bramki wejściowej dla określonego Dokumentu Wejściowego,
- m) pełną dokumentację ruchu osobowego na obiekcie (z datą i czasem sczytania Dokumentu Wejściowego oraz wejścia i wyjścia klienta). System będzie umożliwiać pełny podgląd logów systemowych ze zdarzeń zarejestrowanych w Punktach Kontrolnych dotyczących danego Dokumentu Wejściowego przez Administratora Systemu lub uprawnionego Użytkownika,
- n) obsługę reklamacji z nieudanych wejść na obiekt w Punktach Sprzedaży,
- o) monitorowanie poprawnej pracy Systemu oraz poszczególnych Punktów Kontrolnych.

9.10.3. Sprawdzarki biletowe do bramek obrotowych

Sprawdzarki biletowe będą umożliwiać odczyt następujących rodzajów Dokumentów Wejściowych i znaczników elektronicznych:

- a) kart zbliżeniowych RFID w standardzie MIFARE: ISO14443 A,
- b) biletów papierowych i plastikowych z kodem kreskowym 1D i 2D,
- c) biletów papierowych z elementem RFID (MIFARE),
- d) biletów w systemie print@home,
- e) wirtualnych biletów wstępu z urządzeń mobilnych na podstawie odczytu QR Code.
- f) Biletów elektronicznych – których nośnikiem jest dowód osobisty (odczyt strefy MRZ)

Sprawdzarki biletowe posiadają pamięć wewnętrzną o wielkości bufora dla 25 000 rekordów uprawnionych Dokumentów Wejściowych oraz danych osobowych uprawnionych do wejścia osób a także 50 000 rekordów zapisanych transakcji. Przez transakcję należy rozumieć każde zarejestrowane zdarzenie przez sprawdzarkę biletową. Sprawdzarka biletowa będzie miała możliwość pracy w trybie off-line – sterowanie bramką obrotową na podstawie odpowiedzi z Systemu zarządzającego lub po porównaniu z wewnętrzną listą. Po przywróceniu pracy Systemu do trybu on-line,

sprawdzarki będą umożliwiać uaktualnienie w serwerze zarządzającym Systemu danych zbuforowanych w sprawdzarce w trybie off-line.

Wszystkie sprawdzarki biletowe będą wyposażone w sygnalizację świetlną i dźwiękową, oraz wyświetlacz LCD TFT 7” o rozdzielczości 800x480 pikseli, na którym będą wyświetlane informacje tekstowe i graficzne dla kibica.

Sprawdzarki będą odczytywać i sygnalizować wszystkie rodzaje biletów, w tym bilety zniżkowe i bilety osób poniżej 13-go roku życia oraz sterować bramką obrotową i odbierać z niej sygnał zwrotny umożliwiając zaliczenie biletu na podstawie faktycznego przejścia kibica/osoby.

9.10.4. Sygnalizatory świetlne dla ochrony

Od strony wewnętrznej stadionu w konstrukcji każdego toru wejściowego bramy obrotowej wysokiej będą zainstalowane kolorowe sygnalizatory świetlne dla pracowników ochrony. Będą one współpracować ze sprawdzarką biletową i sygnalizować służbom ochrony status biletu odczytywanego przez sprawdzarkę biletową. Podstawowe komunikaty sygnalizatora:

- ☐ Przesuwająca się zielona strzałka – bilet normalny poprawny
- ☐ Przesuwająca się żółta strzałka – bilet ulgowy poprawny
- ☐ Przesuwająca się niebieska strzałka – bilet poprawny osoby poniżej 13 –go roku życia
- ☐ Pulsujący czerwony znak X – bilet niepoprawny (nie należący do puli danej imprezy, czytany powtórnie lub nieuprawniony do wejścia – tu dodatkowo informacja na wyświetlaczu dla kibica).

Istnieje możliwość skonfigurowania innych schematów na sygnalizatorze świetlnym. Sygnalizatory świetlne ułatwiają służbie ochrony sprawdzenie uprawnień do ulgi oraz sprawdzenie obecności na stadionie opiekuna osoby poniżej 13-go roku życia, a także sygnalizują próby nieuprawnionych wejść na obiekt.

9.11. Organizacja logistyczna imprez i obiektu

9.11.1. Organizacja wejścia na obiekt

Posiadacz konkretnego Dokumentu Wejściowego tylko raz w ciągu całej imprezy będzie mógł przekroczyć bramę obrotową wejściową. Próba kolejnego wejścia do obiektu z wejściówką o tym samym numerze będzie zarejestrowana jako próba nieuprawnionego wejścia, zasygnalizowana odpowiednimi komunikatami alarmowymi na sygnalizatorze świetlnym i wyświetlaczu sprawdzarki biletowej dla Kibica. Ponowne wejście Kibica na obiekt będzie możliwe po uprzednim przyłożeniu biletu do sprawdzarki wyjściowej i faktycznym opuszczeniu obiektu przez Kibica. Rolę sprawdzarek wyjściowych będą pełnić sprawdzarki wyjściowe na wyznaczonych bramach uchylnych.

9.11.2. Identyfikacja kibiców

Zgodnie z ustawą o bezpieczeństwie imprez masowych w przypadku imprez masowych podwyższonego ryzyka niezbędna jest identyfikacja kibiców zarówno na etapie sprzedaży biletów, na etapie wejścia na obiekt, jak i w dowolnym miejscu na obiekcie podczas trwania imprezy masowej.

Identyfikacja na etapie sprzedaży biletów lub wyrabiania Karty Klienta/Kibica będzie polegała na weryfikacji tożsamości kibica na podstawie dokumentu tożsamości, wprowadzenia jego danych do Systemu (minimalny zakres danych to imię, nazwisko, PESEL) oraz opcjonalnie pobrania wizerunku kibica. W przypadku zakupu biletu przez sklep www konieczna będzie po założeniu swojego profilu przez kibica – weryfikacja tożsamości w Punkcie Sprzedaży – po której nastąpi zablokowanie profilu Klienta z jego danymi obowiązkowymi i kibic nie będzie mógł samodzielnie zmienić swoich obowiązkowych danych osobowych w Systemie. W swoim profilu (po zalogowaniu w sklepie www) będzie mógł zmieniać jedynie swoje dane nieobowiązkowe.

Identyfikację kibiców zapewni również powiązanie Modułu Kontroli Biletów i Identyfikacji Kibiców z systemem CCTV poprzez powiązanie numeru biletu oraz danych osobowych właściciela Dokumentu Wejściowego z materiałem wideo rejestrowanym w momencie wejścia kibica na obiekty (stopklatka z momentu sczytania biletu na sprawdzarce biletowej z możliwością odtworzenia – przewinięcia materiału wideo do przodu i do tyłu z momentu wejścia danej osoby do obiektu). Integracja Modułu Kontroli Biletów i Identyfikacji Kibiców z systemem CCTV na obiektach została szczegółowo opisana w innej części niniejszego projektu.

9.11.3. Obsługa specjalnych grup kibiców

Obsługa osób nieletnich

Osoby nieletnie poniżej 13 roku życia, zgodnie z Ustawą mogą uczestniczyć w imprezie masowej podwyższonego ryzyka jedynie pod opieką osoby dorosłej. System pozwala na taką konfigurację, aby sprzedaż biletu dla osoby poniżej 13-go roku życia była możliwa tylko w powiązaniu z zakupem biletu przez jej opiekuna. Istnieje możliwość sprawdzenia w Systemie, kto jest opiekunem osoby nieletniej.

Osoby powyżej 13 roku życia mogą uczestniczyć w imprezie bez opiekuna, lecz podczas zakupu biletu muszą przyjść z opiekunem, który w celu identyfikacji przedłoży swój dowód tożsamości. Osoba nieletnia musi posiadać legitymację szkolną lub dokument tożsamości oraz numer PESEL. System posiada możliwość takiej konfiguracji, aby na etapie zakupu biletu przez osobę nieletnią (13-18 lat) była możliwość przypisania do niej danych opiekuna. Przypisanie danych opiekuna jest definiowane dla danego biletu/imprezy, tak aby przy kolejnym zakupie biletu przez osobę nieletnią System wymuszał konieczność wprowadzenia danych tego opiekuna, który w danym momencie przyszedł z osobą nieletnią zakupić bilet.

System umożliwia przypisanie opiekuna do profilu osoby nieletniej na etapie zakładania profilu i jego weryfikacji oraz składania wniosku o Kartę Klienta/Kibica.

Obsługa kibiców gości

System umożliwia obsługę kibiców gości zgodnie z ustawą o BIM i zapewnieniem pełnej identyfikacji kibica. Dystrybucja biletów dla kibiców gości będzie się odbywać poprzez udostępnienie klubowi macierzystemu kibiców gości - konta Sprzedawcy (loginu i hasła) w Systemie z przypisanymi odpowiednim uprawnieniami do sprzedaży biletów tylko na sektor gości wraz z zapewnieniem pełnej identyfikacji kibiców gości na etapie sprzedaży biletów. Sprzedawca w klubie macierzystym kibiców gości loguje

się do Systemu poprzez przeglądarkę internetową, prowadzi sprzedaż i wydruk biletów dla swoich kibiców. Jeśli taka forma sprzedaży biletów dla kibiców gości będzie z jakiegoś powodu niemożliwa System umożliwi wydruk i przesłanie przed meczem spersonalizowanych biletów do klubu macierzystego kibiców gości wyemitowanych z Systemu na podstawie wcześniej przesłanej przez klub macierzysty kibiców gości i zaimportowanej automatycznie do systemu listy kibiców wraz ze wszystkimi danymi osobowymi.

Obsługa obcokrajowców

System umożliwia wydanie Karty Klienta/Kibica lub sprzedaż Dokumentu Wejściowego dla obcokrajowców nieposiadających numeru PESEL na podstawie innego ważnego dokumentu tożsamości zawierającego unikatowy numer seryjny oraz zdjęcie. System umożliwia obcokrajowcom założenie profilu w Systemie, złożenie wniosku o wydanie Karty Klienta/Kibica oraz zakup Dokumentów Wejściowych na imprezę zarówno w Punktach Sprzedaży na obiekcie jak i poza obiektem, jak też poprzez obcojęzyczną wersję sklepu www.

Obsługa osób niepełnosprawnych

Osoby niepełnosprawne będą wchodzić na stadion poprzez bramki uchylne wyposażone w sprawdzarkę biletową i sygnalizator świetlny.

9.11.4. Rozpatrywanie reklamacji

Zainstalowany na hali i stadionie System CCTV, za pomocą kamer w sposób ciągły będzie monitorować proces wejścia kibiców na obiekt. Oprogramowanie Modułu Kontroli Biletów będzie sprzężone z zainstalowanym na obiektach systemem CCTV w taki sposób, że umożliwi automatyczne wyszukanie zdarzenia (momentu wejścia danego kibica na obiekt – stopklatka z możliwością uruchomienia dalszych lub wcześniejszych sekwencji wideo i zatrzymania materiału wideo na dowolnej klatce, gdzie operator wybierze najlepszy obraz) w kasie reklamacyjnej tylko na podstawie przeczytanego kodu kreskowego lub chipu RFID w postaci listy zanotowanych zdarzeń z Modułu Kontroli Biletów związanych z danym biletem, a po kliknięciu na wybrany rekord przejście do klatki wideo.

Oprogramowanie Modułu Kontroli Biletów będzie wiązać w sposób jednoznaczny i trwały daną klatkę wideo przedstawiającą wizerunek Klienta/Kibica, z zainstalowanego na obiektach systemu CCTV z numerem seryjnym biletu lub w przypadku biletów spersonalizowanych również z jego danymi osobowymi. Rozwiązanie takie będzie umożliwiać nie tylko skuteczne rozpatrywanie reklamacji ale również udostępnianie materiałów na potrzeby organów ścigania (policji, prokuratury).

9.12. Integracja Modułu Kontroli Biletów i Identyfikacji Kibiców z Systemem CCTV

Dla stadionu i hali projektowany jest system CCTV zostanie dostarczony razem z API, które zostanie udostępnione wykonawcy systemu biletowego, umożliwiając wykonanie integracji w zakresie opisanym poniżej. Integracja Modułu Kontroli Biletów i Identyfikacji Kibiców z zainstalowanym na obiektach Systemem CCTV będzie

realizowana na płaszczyźnie serwerowej obu systemów. Moduł Kontroli Biletów otrzyma protokół dostępu do serwera systemu CCTV, skąd będzie mógł na bieżąco pobierać obrazy z kamer CCTV obserwujących bramki wejściowe. Format protokołu dostępu umożliwi pobranie wycinka obrazu obejmującego pojedyncze przejście z oznaczeniem numeru przejścia i czasu zdarzenia w postaci okienka autoodtworzenia. Okienko autoodtworzenia uruchomi się jako stopklatka zgodna z parametrami wywołania oraz będzie zawierać przyciski przewijania do przodu i do tyłu oraz klawisz pauza. Będzie również dostępny klawisz umożliwiający wydruk stopklatki. Obraz wywołany z archiwum będzie taki sam, jak obraz przeglądany na stanowiskach dozoru CCTV.

Udostępnienie API do Modułu Kontroli Biletów i Identyfikacji Kibiców leży po stronie systemu CCTV.

Warunkiem koniecznym do prawidłowej integracji obu systemów jest synchronizacja czasu systemu CCTV z Modułem Kontroli Biletów i Identyfikacji Kibiców. Udostępnienie czasu z systemu CCTV (wskazanie serwera czasu) dla Modułu Kontroli Biletów i Identyfikacji Kibiców leży po stronie systemu CCTV.

9.13. Okablowanie elektryczne i sygnałowe

Ogólne wytyczne do okablowania systemu.

Okablowanie elektryczne

Do prawidłowej pracy Systemu wymagane jest doprowadzenie zasilania 230V AC do następujących punktów:

- ☐ do każdego kołowrotu (kabel zasilający 3x2,5mm²).

Okablowanie strukturalne

Do prawidłowej pracy Systemu wymagane jest doprowadzenie sieci LAN do następujących punktów:

- ☐ do każdego kołowrotu podwójnego (min 3 kable LAN wg specyfikacji jak w pkt. Sieci strukturalnej).

10. System sygnalizacji włamania i napadu

Obiekt zostanie wyposażony w system sygnalizacji włamania w celu zapewnienia bezpieczeństwa osobom przebywającym i pracującym na terenie obiektu. Centrala systemu obsługiwać będzie obszar hali i stadionu.

10.1. Charakterystyka zastosowanych urządzeń

Centrala alarmowa posiadać będzie certyfikat Grade III (trzy), Klasę środowiskową II.

Klasa środowiskowa II – środowisko wewnętrzne ogólne:

Wpływy środowiskowe występujące zazwyczaj wewnątrz pomieszczeń, gdy nie jest utrzymywana odpowiednia temperatura (np. w korytarzach, holach lub na klatkach schodowych oraz w miejscach, gdzie może wystąpić kondensacja pary na oknach, a

także w nieogrzewanych przestrzeniach magazynowych lub w dużych magazynach, gdzie ogrzewanie jest okresowe).

Przewidywane zmiany temperatury między -10°C a $+40^{\circ}\text{C}$.

10.2. Charakterystyka ogólna systemu

W czujki zostały wyposażone pomieszczenia w budynku zgodnie z częścią graficzną.

Organizacja oznakowania, adresowania, opisywania poszczególnych elementów systemu ma precyzyjnie określać miejsca, z którego otrzymujemy alarm włamaniowy, napad, awarie oraz lokalizacje każdego elementu. System zostanie wyposażony w aplikacje do programowania, zarządzania i administrowania z zainstalowanym oprogramowaniem na jednostce komputerowej.

Do sygnalizacji napadu projektuje się stałe przyciski antynapadowe (pomieszczenia kas).

Włączenie i wyłączenie do dozoru poszczególnych stref ochrony będzie realizowane za pomocą klawiatury z pom. ochrony (obszar hali).

Typ central to mikroprocesorowy układ z własnym zasilaniem awaryjnym. Ochrona obiektu i stref będzie realizowana przy pomocy czujników podczerwieni.

System będzie posiadał możliwość adresowania elementów indywidualnie i grupowo oraz będzie wyposażony w układy antysabotażowe.

11. System kontroli dostępu

Do wybranych pomieszczeń wewnątrz obiektu projektuje się system kontroli Dostępu, zgodnie z częścią graficzną. Platforma systemu będzie wspólna dla obszaru hali i stadionu.

Zaprojektowano zależność systemu SKD z systemem SAP. W przypadku zagrożenia pożarowego wszystkie kontrolowane przez system SKD przejścia, na drodze ewakuacyjnej, zostaną zwolnione, umożliwiając tym samym przeprowadzenie sprawnej ewakuacji.

11.1. System kontroli dostępu - wymagania

- System kontroli dostępu umożliwia sterowanie drzwiami za pomocą czytnika karty zbliżeniowej oraz stacji roboczej systemu kontroli dostępu,
- Czytnik karty zbliżeniowej pracuje zgodnie z MiFare DESFire EV1,
- System kontroli dostępu obsługuje jednocześnie maks. cztery (4) różne formaty karty Wiegand. Liczba wszystkich obsługiwanych formatów jest nieograniczona,
- Utrata komunikacji pomiędzy oprogramowaniem zarządzającym a kontrolerami nie powinna mieć wpływu na normalne działanie systemu,
- System kontroli dostępu jest zaprojektowany w taki sposób, aby awaria dowolnego kontrolera w systemie nie miała wpływu na normalne działanie pozostałych kontrolerów,
- System kontroli dostępu powinien posiadać świadectwo dopuszczenia CNBOP,

- System kontroli dostępu oferuje konfigurowalne harmonogramy czasowe umożliwiające elastyczne programowanie automatycznego blokowania i odblokowania dowolnych drzwi, a także włączanie i wyłączanie ustawień posiadacza karty w celu ograniczenia możliwości wejścia do określonych obszarów dla dowolnej grupy dostępu w zaprogramowanych godzinach,
- Harmonogram czasowy zawiera funkcję dni świątecznych umożliwiającą użytkownikowi programowanie świąt narodowych oraz definiowanie własnych świąt,
- Wszystkie harmonogramy są definiowane w oparciu o dzień, godziny i minuty.

11.2. Hardware systemu

- System kontroli dostępu powinien być rozbudowywalny do przynajmniej 1200 czytników,
- Komunikacja sterowników kontroli dostępu z serwerem zarządzającym powinna odbywać się za pomocą TCP/IP,
- Sterowniki systemu kontroli dostępu w przypadku utraty połączenia z serwerem (praca offline / autonomiczna) zarządzającym powinny realizować swoje funkcje normalne,
- Podczas pracy offline, każdy sterownik kontroli dostępu powinien być w stanie przechować przynajmniej 1 000 000 zdarzeń (jeden milion), które w momencie powrotu komunikacji z serwerem, będą wysłane do bazy danych oprogramowania zarządzającego,
- Sterowniki kontroli dostępu powinny monitorować status zasilania baterijnego, zasilania sieciowego AC oraz napięcia DC między zasilaczem a samym sobą. Wspomniane informacje powinny być raportowane do oprogramowania zarządzającego,
- Sterowniki kontroli dostępu powinny mieć możliwość pracy w sieci LAN oraz WAN,
- Każdy sterownik powinien być wyposażony w wejścia służące do obsługi np. kontaktronów, przycisków wyjścia uprawnionego oraz w wyjścia przekaźnikowe do np. sterowania drzwiami,
- Każde wyjście przekaźnikowe w sterowniku powinno mieć możliwość niezależnej konfiguracji pracy bezpotencjałowej,
- Każde wejście powinno posiadać możliwość parametryzacji przy pomocy dwóch rezystorów,
- Sterownik kontroli dostępu obsługuje połączenia z maksymalnie 4 standardowymi czytnikami z interfejsem Wiegand lub 8 czytnikami z interfejsem szeregowym działającymi na magistrali RS-485.

11.3. Software

- Oprogramowanie zarządzające systemem kontroli dostępu powinno pracować w architekturze klient-serwer,
- Aplikacja serwerowa powinna wspierać architekturę 32bit oraz 64bit,

- Oprogramowanie systemu kontroli dostępu powinno wspierać standardy IT takie jak OPC, AutoCAD, LDAP, HTML, ASP.NET,
- Oprogramowanie powinno rejestrować zdarzenia w bazie danych MSSQL,
- Oprogramowanie powinno mieć możliwość wyboru, jakie typy zdarzeń mają być rejestrowane w bazie MSSQL,
- Oprogramowaniem zarządzające powinno mieć możliwość współpracy z bazą danych MSSQL zainstalowaną na tym samym komputerze jak również na komputerze zdalnym (taka konfiguracja może być podyktowana wydajnością serwerów),
- Wizualizacja
 - Wizualizacja elementów systemu kontroli dostępu powinna być realizowane w oparciu o mapy wektorowe np. AutoCad
 - Z poziomu mapy wizualizacyjnej operator powinien mieć łatwy dostęp do komend sterujących jak:
 - Otwórz drzwi jednorazowo,
 - Otwórz drzwi na stałe,
 - Zablokuj drzwi,
 - Zablokuj czytnik,
 - Wysteruj przekaźnik,
 - Pokaż ostatnie zdarzenia jakie miały miejsce na urządzeniu,
 - Ikony przedstawiające poszczególne elementy systemu (drzwi, czytniki, sterowniki) powinny być możliwe do zmiany,
- Interfejs graficzny operatora
 - Powinien być edytowalny w celu dostosowania go do potrzeb i uprawnień operatora,
 - Powinna być możliwość dodania przycisków wykonujących wybrane komendy na wybranej grupie urządzeń,
- System powinien mieć możliwość alarmowania przynajmniej o:
 - Wyważeniu drzwi,
 - Zbyt długim otwarciu drzwi,
 - Utracie komunikacji z dowolnym sterownikiem,
 - Użycie karty z czarnej listy,
 - Użycie karty bez uprawnień,
 - Użycie karty nieznanej,
 - Użyciu karty o określonym numerze,
 - Błędny kod PIN,
 - Karta poza trasą,
 - Alarm sabotażowy sterownika,
 - Antipassback,
 - Ważność uprawnień wygasła,
 - Wrywkowa kontrola,
- Oprogramowanie w momencie wykrycia istotnego zaprogramowanego zdarzenia alarmowego powinno mieć możliwość:

- Powiadomienia operatora sygnałem dźwiękowym,
- Automatycznego wykonania zbliżenia na mapie na urządzenie, które jest w stanie alarmu,
- Wyświetlenia dokumentu alarmowego np. z procedurą postępowania na wypadek danej sytuacji,
- Wyświetlenie dodatkowej warstwy graficznej na mapie na wizualizacyjnej np. dróg ewakuacyjnych na wypadek pożaru,
- Wykonać komendy sterujące (np. Zablokować drzwi,ysterować przekaźnik),
- Oprogramowanie powinno zapewniać możliwość definiowania obszarów logicznych w obiekcie (np serwerownia, biuro itd) w celu monitorowania położenia posiadaczy kart,
- Kolejność przejść - system powinien udostępniać funkcję sprawdzania kolejności dostępu, która umożliwia uprawnionemu posiadaczowi karty wejście przez drzwi lub grupę drzwi należącą do zdefiniowanego obszaru tylko, kiedy osoba przeszła już przez inne określone drzwi,
- Śluza – system powinien posiadać funkcję śluzy umożliwiającą zarządzanie dwoma lub więcej powiązаныmi drzwiami sterowanymi przez dwie pary lub więcej czytników (we / wy) lub czytniki wejścia oraz przycisk żądania wyjścia. W tym samym momencie mogą być otwarte tylko jedne drzwi. Tak długo jak jedne drzwi są otwarte, pozostałe będą zablokowane przed dostępem,
- Uprawnienia operatora
 - Oprogramowanie powinno umożliwiać skonfigurowanie indywidualnych uprawnień operatora
 - Uprawnienia odnoście danych użytkowników:
 - Widoczność,
 - Odczyt,
 - Modyfikacja,
 - Usuwanie,
 - Dodawanie,

Wyjaśnienie: powinna być możliwość tak skonfigurowania uprawnień operatora, aby mógł tylko odczytać określone dane użytkownika i je zmodyfikować ale, aby nie mógł usunąć karty.

- Uprawnienia odnośnie komunikowanych zdarzeń do operatora:
 - Pokaż własne komunikaty,
 - Pokaż komunikaty bez danych osobowych,
 - Pokaż wszystkie komunikaty,
- Uprawnienia odnośnie widocznych na mapie wizualizacyjnej elementów,
- Uprawnienia odnośnie widocznych map wizualizacyjnych.

11.4. Urządzenia wchodzące w skład SKD

Kontroler:

Modułowy kontroler dostępu do systemu kontroli dostępu. Urządzenie kontroluje od

jednego do ośmiu punktów dostępu, może sprawować kontrolę nad maksymalnie ośmioma czytnikami kart identyfikacyjnych (zależnie od typu czytników) i został zaprojektowany do kompletnego przetwarzania danych dostępowych w przypisanych lokalizacjach.

Kontrolę stanu można przeprowadzać, korzystając z ośmiu wejść analogowych. Ośmiem wyjść przekaźnikowych służy do uruchamiania siłowników drzwi i / lub aktywacji systemu bezpieczeństwa i sygnalizacji alarmowej. Kontroler przechowuje wszystkie potrzebne informacje w podtrzymywanej akumulatorowo pamięci oraz na karcie CompactFlash, co pozwala na przeprowadzanie niezależnych kontroli autoryzacji w punktach dostępu, podejmowanie decyzji o dostępie, sterowanie siłownikami oraz rejestrowanie zdarzeń przejścia nawet w przypadku utraty połączenia z komputerem. Kontrolery będą podłączane do systemu za pomocą sieci Ethernet.

Podstawowe funkcje kontrolera:

- Przechowywanie poniższych danych:
 - Dane główne
 - Autoryzacje
 - Uprawnienia dostępu
 - Wyświetlany tekst
 - Konfiguracje czytników
- Interpretacja danych transakcji z czytnika
 - Kontrola autoryzacji
 - Żądania komputera
 - Kod PIN
- Kontrola / monitoring
 - Brak zezwolenia lub zezwolenie na wejście
 - Wyzwalanie alarmu
 - Stany drzwi
 - Stany pracy czytników
 - Stany alarmu wewnętrznego
- Wysyłanie komunikatów do systemu Access Engine
 - Żądania komputera
 - Dane transakcji do zachowania
 - Komunikaty o błędach i usterkach
 - Komunikaty alarmowe
- Dostarczanie zasilania dla następujących elementów:
 - Czytniki
 - Siłowniki drzwi
 - Zaciski do zasilania styków

Czytnik kart:

- Środowisko pracy: w pomieszczeniach i na zewnątrz — każde warunki atmosferyczne.

- Temperatura pracy -25°C do 65°C (-13°F do 150°F)
- Wilgotność podczas pracy 0 do 95% (bez kondensacji)
- Stopień ochrony IP65
- Odporność na promieniowanie UV Tak
- Dane techniczne MIFARE i kart:
 - Zasięg odczytu — karty ISO > 3 cm
 - Pilot > 2 cm
 - Obsługiwane karty MIFARE 13,56 MHz ISO 14443, typ A
 - Zabezpieczenie antykolizyjne Tak
 - Obsługa układów scalonych NXP: MF3ICD21 — 2K MF3ICD41 — 4K MF3ICD81 — 8K

12. System integracji

Oprogramowanie (Building Integration System) pozwala na współpracę systemów CCTV, SAP, SKD, SSWiN i na optymalny ogląd sytuacji. Dzięki temu możliwe staje się natychmiastowe reagowanie na pojawiające się zdarzenia. Platforma oprogramowania wspólna dla hali i stadionu.

Oprogramowanie tworzy bazę pozwalającą na integrację wielu systemów, w tym między innymi sygnalizacji pożaru, sygnalizacji włamania i napadu, monitoringu, kontroli dostępu. Łączy systemy za pomocą interfejsów wysokiego poziomu w jeden spójny system bezpieczeństwa z jednym interfejsem użytkownika.

Zaprojektowane oprogramowanie BIS lub równoważne łączy funkcje kompleksowego wideodozoru i kontroli dostępu. Zapewnia personelowi ochrony optymalny ogląd sytuacji i pozwala na skuteczniejsze reagowanie na rejestrowane zdarzenia. Jeśli na przykład system wykryje pozostający bez opieki bagaż, można natychmiast zarządzić ewakuację. Można też otworzyć dodatkowe wyjścia awaryjne, jeżeli po ogłoszeniu alarmu pojawi się zator przy jednych drzwiach. Błyskawiczną reakcję na pojawiające się zdarzenia umożliwia funkcja inteligentnej analizy obrazu, która zapewnia dodatkowe kryteria monitoringu umożliwiające lepszą ocenę sytuacji.

BIS umożliwia równoczesną obsługę i monitoring wszystkich systemów bezpieczeństwa i kontroli w danym obiekcie. Zwiększa szybkość reagowania i usprawnia działanie w nagłych przypadkach. Pozwala na lepszą koordynację sygnałów alarmowych i zapisów wideo. W przypadku integracji z systemem kontroli dostępu, może przetwarzać większą liczbę równocześnie pojawiających się danych, na przykład skanowanych kart dostępu.

Standardowe formaty:

- OPC
- Do konfiguracji AutoCAD, HTML, XML
- Do wyświetlania HTML, ASPX, IE, web server based
- Do sieciowania IIS web server, TCP/IP environment

Standardowe systemy operacyjne:

- Windows XP SP3
- Windows 7
- Windows 2003 Server
- Windows 2008 Server

Architektura sprzętowa:

- 32 bit
- 64 bit

Podstawowe funkcje oprogramowania:

- zarządzanie systemem Kontroli Dostępu z ponad 128 czytnikami,
- wizualizacja w oparciu o mapy CAD (np. systemu SAP)
- pełna integracja systemów: KD, CCTV, SAP, DSO, SSWiN,
- budowa scenariuszy sytuacyjnych,
- wyświetlanie dokumentów jak np. procedury postępowania w określonej sytuacji,
- system działający w oparciu o bazę danych SQL,
- funkcjonalność nie będąca standardową funkcją żadnego z systemów,
- dostosowanie wyglądu interfejsu,
- wydzielenie niezależnych stref systemu wraz z przynależącymi do nich grupami użytkowników (obiekt z wieloma najemcami),
- możliwość integracji z systemami innych producentów po przez OPC.

12.1. Warstwa sprzętowa

W szafie GPD w hali zainstalowany zostanie serwer. Na serwerze zostanie zainstalowane oprogramowanie BIS.

Stacje komputerowe ujęte w projekcie CCTV, stanowią jednocześnie jednostki PC na których będzie / może być sprawowana obsługa systemu BIS.

13. System videodomofonowy i interkomowy

Dla umożliwienia komunikacji pomiędzy użytkownikami a innymi służbami lub petentami, zostanie zaprojektowany system videodomofonowy oraz interkomowy. Panele systemu zlokalizowano zgodnie z częścią graficzną. W pomieszczeniu ochrony (obszar hali) zaprojektowany zostanie panel odbiorczy.

14. Instalacja RTV

W części graficznej zaznaczono miejsca instalacji gniazdek RTV. Projektuje się dystrybuowanie sygnału naziemnej TV w instalacji.

15. System sygnalizacji pożaru

System detekcji pożaru zaprojektowano w zakresie ochrony całkowitej dla pomieszczeń podlegających ochronie.

W pomieszczeniu 0-133 (Centrum dowodzenia akcją gaśniczą) w obszarze Hali,

zlokalizowane zostaną urządzenia sterujące i nadzorujące pracę systemów bezpieczeństwa pożarowego.

System będzie pracował w układzie sieci central pożarowych dla dwóch obiektów tj Hali i Stadionu.

W obszarze Stadionu zaprojektowano dwie centrale SAP:

- W pom. [0]-S-Z-01 serwerownia,
- W pom. [+2]-S-F-01 Centrum kontroli i dowodzenia Strefa dowodzenia.

Zadaniem projektowanego systemu ostrzegania o pożarze jest ciągle monitorowanie pomieszczeń w ramach obiektu, pod kątem wykrycia dymu i ognia w jak najwcześniejszym stadium. Ponadto zapewnia on szybkie i precyzyjne przekazanie informacji o zdarzeniu alarmowym do centrum monitorowania lub systemu nadzoru.

System automatycznego wykrywania i ostrzegania przed pożarem jest zbudowany z następujących elementów:

- adresowalnych central pożarowych / centrali pożarowej,
- adresowalnych czujek,
- wskaźników zadziałania czujek zamontowanych w niewidocznych miejscach np. w przestrzeni międzysufitowej,
- certyfikowanych zasilaczy,
- certyfikowanych puszek połączeniowych PIP dla rozgałęzień przewodów o odporności ogniowej,
- adresowalnych ręcznych ostrzegaczy pożarowych,
- Modułów sterujących (wejścia/wyjścia).

Informacja o alarmie powinna zawierać dokładną lokalizację pożaru w postaci adresu alarmującego elementu oraz opisu pomieszczenia / obszaru (na wyświetlaczu ciekłokrystalicznym i na wydruku wbudowanej drukarki protokołującej).

Jednocześnie poprzez urządzenie transmisji alarmu powiadomienie o pożarze (alarm II stopnia) przesłane zostanie automatycznie do Państwowej Straży Pożarnej.

Projektuje się system sygnalizacji pożarowej, pracujący w układzie linii dozoruowych pętlowych z indywidualnym adresowaniem następujących elementów liniowych:

- czujek adresowalnych (automatycznych, ręcznych),
- modułów sterujących we/wy.

Wszystkie zaprojektowane w systemie elementy pracujące w pętłach dozoruowych muszą posiadać obustronne izolatory zwarć dla uzyskania wysokiej odporności systemu na uszkodzenia typu „przerwa” lub „zwarcie” w pętli dozoruowej.

Pełna adresowalność instalacji sygnalizacji pożarowej umożliwiać będzie m. in. identyfikację miejsca pożaru z dokładnością do pojedynczego punktu adresowego, tj. czujki, modułu sterującego, a także możliwość programowego przypisania funkcji wykonawczych (sterujących) i funkcji monitorujących poszczególnym adresowanym wyjściom sterującym i wejściom monitorującym w modułach włączonych w pętle dozoruowe i zainstalowanych w obiekcie. Nie przewiduje się zastosowania w obiekcie czujek z izotopem promieniotwórczym.

Projektowany system jest zgodny z normami europejskimi oraz rekomendacją techniczną PKN-CEN/TS 54-14 i stosownymi wytycznymi Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej (CNBOP) w Józefowie i/lub Instytutu Techniki Budowlanej w Warszawie. System posiada aktualny certyfikat zgodności zgodnie z dyrektywą budowlaną (znak B lub CE) oraz świadectwo dopuszczenia CNBOP.

System sygnalizacji alarmowania pożarowego - główne cele, specyfikacja urządzeń

System sygnalizacji pożarowej jest zaprojektowany w oparciu o normę PN-EN 54 i specyfikację techniczną PKN-CEN/TS 54-14:2006.

Zadaniem projektowanego systemu ostrzegania o pożarze jest ciągle monitorowanie pomieszczeń w ramach obiektu, pod kątem wykrycia dymu i ognia w jak najwcześniejszym stadium. Ponadto zapewnia on szybkie i precyzyjne przekazanie informacji o zdarzeniu alarmowym do centrum monitorowania lub Państwowej Straży Pożarnej (PSP).

Z central wyprowadzono niezależne pętlowe linie dozоровe, które obsługiwać będą pomieszczenia oraz korytarze na wszystkich kondygnacjach budynku. Dzięki zastosowaniu linii pętlowej eliminujemy uszkodzenia w instalacji w postaci przerwy lub zwarcia obwodu.

Czujki pożarowe zostaną umieszczone we wszystkich pomieszczeniach w budynku jak i na korytarzach, klatkach schodowych. Zastosowanie czujek pożarowych zostało podyktowane warunkami wewnątrz chronionych pomieszczeń: wyposażeniem, przewidywanym sposobem palenia się materiałów itd.

Informacje o elemencie znajdującym się w stanie alarmu będą wyświetlane w centrali.

Projektuje się podawanie następujących danych:

- nazwa pomieszczenia w którym jest zainstalowany ostrzegacz znajdujący się w stanie alarmu,
- nazwa strefy wykrywania,
- data i godzina alarmu.

Projekt przewiduje wykorzystanie do ochrony obiektu linii dozоровych posiadających rezerwy dla dołączenia ewentualnych dodatkowych ostrzegaczy dla rozbudowy systemu i dołączenie innych pomieszczeń obiektu. W przypadku zaniku napięcia w sieci elektroenergetycznej 230VAC lub uszkodzenia zasilacza pracę systemu umożliwiają akumulatory bezobsługowe wbudowane w szafkę centrali. Zapewniają one prawidłową pracę systemu w stanie dozоровania w ciągu minimum 30 godz. bez zasilania podstawowego oraz po upływie tego czasu minimum 0,5 godz. w stanie alarmowania. Wszystkie główne połączenia w systemie są stale nadzorowane od zwarc i przerw przewodu, tak że uszkodzenie jest natychmiast sygnalizowane obsłudze.

Informacje o urządzeniu znajdującym się w stanie alarmu będą wyświetlane w centrali.

Ręczne przyciski sygnalizacji p.poż. instalowane będą na wysokości 1,4m od poziomu podłogi.

W obiekcie przyjęto wariant alarmowania dwustopniowego.

Promień działania czujki pożarowej dla projektowanego obiektu nie może być większy niż 7,5m. Minimalne odległości czujek pożarowych, jakie należy zachować w czasie montażu są następujące:

- od ścian i podłogi – 0,5m,
- opraw świetlówkowych (dławików) – 0,5m.

Projekt przewiduje, że jako przewody linii dozorowych, wewnątrz obiektu, należy zastosować przewód YnTKSY 1x2x0,8mm. Przewód należy prowadzić w rurkach instalacyjnych natynkowo, głównych trasach - metalowych korytach, bądź prowadząc instalację w tynku. Do „pierwszego” i „ostatniego” elementu na pętli dozorowej należy doprowadzić, wewnątrz budynku, przewód niepalny HTKSH 1x2x0,8mm PH90. Przewody te należy prowadzić w trasach kablowych posiadających odporność ogniową PH90 lub na certyfikowanych uchwytach montażowych.

Zastosowane urządzenia muszą posiadać certyfikaty, świadectwa dopuszczenia obowiązujące na terenie Polski.

15.1.1. Organizacja alarmowania systemu

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 budynku przyjęto dwustopniową procedurę organizacji alarmowania. Przy tak przyjętej procedurze zagrożenie wykryte przez czujkę automatyczną powoduje jedynie sygnalizację alarmu pożarowego I stopnia. Od momentu zgłoszenia alarmu odliczany jest czas potwierdzenia obecności obsługi, a następnie po potwierdzeniu przez obsługę przyjęcia z centrali informacji, odliczany jest czas rozpoznania. Jeżeli przed upływem czasu rozpoznania nie zostaną podjęte żadne czynności (potwierdzenie lub skasowanie) system sygnalizacji pożarowej automatycznie przechodzi w alarm II stopnia.

Czasy zweryfikować na obiekcie w trakcie testów i po uzgodnieniu ze służbami Zamawiającego.

Alarm pożarowy I stopnia

Jest to alarm sygnalizowany jedynie na wyniesionych polach obsługi centrali pożarowej. Alarm może zostać wygenerowany przez dowolną czujkę automatyczną (wskazywana jest wtedy dokładna lokalizacja miejsca wystąpienia zagrożenia pożarowego).

Alarm pożarowy II stopnia

System sygnalizacji pożarowej po upływie czasu potwierdzenia lub rozpoznania automatycznie przechodzi w alarm II stopnia. Wywołanie alarmu II stopnia powoduje bezzwłoczne wysłanie komunikatu o zagrożeniu pożarowym za pośrednictwem urządzeń transmisji alarmów do najbliższej lokalnej jednostki Państwowej Straży Pożarnej. Dodatkowoysterowane zostają urządzenia automatyki pożarowej odpowiedzialne za utworzenie wydzieleni pożarowych i uszczelnienie pożarowe

budynku, uruchamiane sygnałem ogólnym alarmu II stopnia, (czyli niezależnie od miejsca powstania zagrożenia), a takżeysterowanie urządzeń odpowiedzialnych za sprawną i bezpieczną ewakuację z zagrożonej strefy.

Czas potwierdzenia

Po zgłoszeniu przez system SAP alarmu I stopnia, służby dozoru mają obowiązek potwierdzenia przejęcia informacji o zagrożeniu pożarowym oraz o podjętej interwencji. Przyjęto, że czas potwierdzenia wynosi 30 sekund. W tym czasie pracownik ochrony dozoru w pomieszczeniu ochrony musi podejść do konsoli i wcisnąć przycisk ROZPOZNANIE. Po upływie czasu potwierdzenia bez wciśnięcia przycisku ROZPOZNANIE ze strony obsługi, system przechodzi w alarm II stopnia. Brak potwierdzenia alarmu w wyznaczonym czasie jest równoznaczne z brakiem możliwości podjęcia przez służby dozoru interwencji. Ma to szczególne znaczenie w przypadku, gdy pożar wystąpił w pomieszczeniu ochrony i służby dozoru nia są w stanie realizować określonych procedur.

Czas rozpoznania

Po potwierdzeniu przez służby dozoru alarmu I stopnia następuje odliczanie czasu niezbędnego na dotarcie do miejsca wystąpienia zagrożenia pożarowego i określenia jego stopnia. Przyjęto czas rozpoznania 3 minuty. W tym czasie pracownik służb dozoru po dotarciu na miejsce zagrożenia podejmuje decyzję o konieczności wezwania Jednostek Ratunkowych PSP lub próbie neutralizacji zagrożenia we własnym zakresie. W pierwszym przypadku niezbędne jest wciśnięcie najbliższego ROPa lub przekazanie informacji do pracownika pełniącego dozór przy konsoli w celu wciśnięcia ROPa zlokalizowanego w pomieszczeniu ochrony. W przypadku możliwości podjęcia akcji gaśniczej we własnym zakresie niezbędne jest zablokowanie wywołania alarmu II stopnia poprzez skasowanie alarmu lub zablokowanie elementu alarmującego przed upływem 3 minut. W przypadku braku jakiejkolwiek reakcji (potwierdzenie ROPem lub skasowanie alarmu) po 3 minutach system przechodzi automatycznie w alarm II stopnia. Szczegóły działania służb dozoru przy centrali w budynku użytkownik określi wewnętrznymi procedurami organizacyjnymi.

15.1.2. Automatyczne powiadamianie PSP

System umożliwia połączenie z lokalną jednostką Państwowej Straży Pożarnej za pośrednictwem urządzenia transmisji alarmów (UTA). Z nadajnikiem UTA centrala SAP powinna zostać połączona bezpośrednio przewodami uniepalnionymi YnTKSY. Centrala umożliwia przesyłanie sygnałów alarmu ogólnego II stopnia, sygnałów alarmów z poszczególnych stref oraz sygnału ogólnego uszkodzenia systemu poprzez zamknięcie odpowiednich styków przekaźnika w centrali sygnalizacji pożarowej.

Sposób transmisji sygnałów z UTA do stacji monitoringu oraz sam nadajnik UTA dostarczany jest przez firmę specjalizującą się w monitoringu i transmisji alarmów. Obowiązek podpisania stosownej umowy z firmą monitorującą leży po stronie użytkownika obiektu. Nadajnik UTA powinien przekazywać, co najmniej:

- 1. alarm pożarowy,
- 2. awarię zbiorczą systemu SAP.

15.1.3. Konfiguracja systemu i dobór urządzeń

W części graficznej, na planach instalacyjnych, przedstawiono lokalizację podstawowych elementów systemu, a także lokalizację głównych urządzeń sterowanych i monitorowanych przez system SAP.

15.1.4. Ogólny opis

Centrala sygnalizacji pożarowej należy do urządzeń analogowych typu adresowalnego. Automatyczne czujki pożarowe oraz ręczne ostrzegacze pożarowe, które zapewniają wykrywanie pożaru, są przyłączone w zamkniętych pętlach do centrali sygnalizacji pożarowej i są identyfikowane jako pojedyncze elementy. W zależności od struktury budynku czujki i ręczne ostrzegacze pożarowe mogą być pogrupowane softwareowo w logiczne strefy. Centrala sygnalizacji pożarowej może zarządzać co najmniej 32.000 różnych stref.

Centrala sygnalizacji pożaru została zbudowana jako całkowicie modułowa przy użyciu modułów, które są wpinane na szynie. Niemożliwe jest, aby moduł wpiąć niepoprawnie na szynie. Szyna ta zapewnia modułom zasilanie i komunikację z kontrolerem wewnętrznym centrali. Miejsce, w którym dany moduł zostanie wpięty na szynie może być wybrane całkowicie losowo w zależności od wymagań funkcjonalnych danej instalacji. Centrala sygnalizacji pożarowej może być wyposażona w sumie w 46 modułów, z których co najmniej 32 może być analogowymi adresowalnymi modułami pętlowymi.

Moduły posiadają obudowę z plastiku, która zabezpieczenia podzespoły elektronicznie przed czynnikami zewnętrznymi. W przypadku uszkodzenia lub problemów z danym modułem, może on być wymieniony bez konieczności odłączania zasilania lub przeprogramowania centrali sygnalizacji pożarowej.

Okablowanie np. pętli jest przyłączane do zdejmowalnych zacisków, które są wpinane do modułów. Każde połączenie jest oznakowane.

Centrale sygnalizacji pożarowej powinny spełniać wymagania normy PN-EN 54-2 oraz normy PN-EN 54-4.

15.1.5. Moduły funkcjonalne centrali

Moduły funkcjonalne są autonomicznymi urządzeniami typu „plug-and-play”, które można umieścić w dowolnym slotcie centrali. Moduł jest automatycznie identyfikowany przez centralę i działa w trybie domyślnym. Zasilanie i wymiana danych z centralą odbywa się automatycznie, za pośrednictwem szyn przyłączeniowych, bez konieczności dodatkowych ustawień. W przypadku awarii któregośkolwiek z modułów istnieje możliwość wymiany poszczególnych modułów funkcjonalnych bez konieczności wyłączania całego systemu oraz ponownego programowania centrali po wymianie modułów.

Moduł sieci LSN lub równoważny umożliwia dołączenie pętli LSN o długości do 1000m zawierającej maksymalnie 254 elementy (punkty detekcji) o maksymalnym natężeniu prądu wyjściowego 300mA. W pojedynczych przypadkach istnieje możliwość dołączenia pętli o długości do 3000m zawierającej 254 elementy o maksymalnym

natężeniu prądu wyjściowego do 1500mA.

Moduł przekaźników zawiera osiem przekaźników z zestykiem przełącznym (typu C), które zapewniają beznapięciowe styki wyjściowe do przełączania zewnętrznych obciążeń. Każdy z ośmiu przekaźników posiada styk normalnie otwarty (NO) i normalnie zamknięty (NC). Maksymalne obciążenie styku przekaźnika wynosi 1A / 30VDC.

Moduł kontroli akumulatorów monitoruje zasilanie całej centrali i reguluje, sterowane czasowo i temperaturowo, ładowanie maksymalnie czterech akumulatorów 12V / 40Ah lub 12V/28Ah. Ładowanie akumulatorów jest uruchamiane ręcznie za pomocą przycisku. Moduł zawiera wskaźniki LED wskazujące obecność zasilania z sieci, awarii sieci i awarii akumulatorów.

Moduł komunikacyjny wyposażony jest w interfejs S1 dialera, interfejs RS232 drukarek szeregowych oraz interfejs S20 umożliwiający dołączenie drukarki raportów.

15.1.6. Kontroler centrali sygnalizacji pożarowej

Moduły wpinane na szynę centrali sygnalizacji pożarowej są obsługiwane przez kontroler wewnętrzny. Firmware, dane konfiguracyjne oraz wszystkie ustawienia są przechowywane w pamięci flash kontrolera. Dane konfiguracyjne oraz ustawienia są przechowywane również w modułach wpiętych na szynę. Uszkodzenie lub brak modułu może być sprawdzony poprzez panel dotykowy kontrolera centrali.

Kontroler Centrali jest standardowo wyposażony w wielokolorowy graficzny panel dotykowy, za pomocą którego można obsługiwać cały system sygnalizacji pożarowej. Panel dotykowy LCD ma średnicę 14,5cm oraz rozdzielczość 320x240 pikseli. Czytelność tekstu na ekranie jest zapewniona poprzez podświetlenie z tyłu. Użytkownik może zmieniać ustawienia kontrastu. Kontroler centrali powinien być wyposażony w co najmniej 11 czerwony, żółtych i zielonych diod LED, które sygnalizują stan pracy centrali sygnalizacji pożarowej.

Panel dotykowy prezentuje w przejrzysty sposób informacje o alarmie pożarowym, uszkodzeniu itp. Wbudowany brzęczyk może być aktywowany (ton ciągły lub modulowany) w celu wzbudzenia zainteresowania obsługi obiektu w przypadku jakiegoś zdarzenia. Każde zdarzenie musi być potwierdzone przez obsługę. Po potwierdzeniu brzęczyk jest wyciszany. Na panelu dotykowym wyświetlane są następujące informacje w przypadku wystąpienia zdarzenia: adres logiczny, czytelny opis strefy logicznej oraz miejsca detekcji zdarzenia (32 znaki).

Na tym samym ekranie obsługa ma możliwość skasowania alarmu lub uruchomienia alarmu II stopnia (ewakuacyjnego). W dolnej części panelu dotykowego znajduje się pasek stanu, na którym wyświetlane są ogólne informacje na temat aktualnych zdarzeń. Obsługa centrali sygnalizacji pożarowej odbywa się za pomocą intuicyjnego menu. Użytkownik przyciska palcem panel dotykowy LCD, porusza się po menu i wybiera interesujące funkcje.

Następujące funkcje mogą być wyzwolone co najmniej przy pomocy panelu dotykowego:

- skasowanie 1 czujki, strefy dozoru lub całego systemu,
- wyłączenie brzęczyka

- wyciszenie sygnalizatorów akustycznych
- włączenie oraz wyłączenie bypassu/blokowania czujek lub grupy czujek
- przełączanie trybu pracy dzień/noc
- przeglądanie informacji z licznika zdarzeń
- ustawianie daty i godziny
- przełączenie czujek/grup czujek w tryb testowania
- zmiana profilu detekcji wielokryteriowych czujek pożarowych
- zmiana opisu strefy logicznej lub miejsca detekcji

Wszystkie zdarzenia są przechowywane w pamięci zdarzeń (liczniku zdarzeń). Licznik zdarzeń ma pojemność 10000 zdarzeń i jest przechowywany w pamięci flash kontrolera centrali. W przypadku kompletnego uszkodzenia zasilania zdarzenia pozostaną zapisane w pamięci.

Każde zdarzenie jest przechowywane wraz z:

- unikalnym numerem
- datą i godziną wystąpienia
- adresem logicznym elementu lub miejsca detekcji
- opisem elementu lub miejsca detekcji

Przy użyciu menu użytkownika możliwe jest odczytywanie pamięci zdarzeń w chronologicznym porządku.

W celu wyszukiwania konkretnych informacji można użyć opcji filtrowania w zakresie danego:

- Zdarzenia
- Przedziału czasowego
- Elementu/miejsca detekcji

Wersja językowa jest niezwłocznie ustawiana zgodnie z wyborem użytkownika bez konieczności restartu centrali.

Użytkownicy mogą zostać podzieleni na 4 różne grupy. W zależności od poziomu użytkownika ustalany jest dostęp do danych funkcji. Funkcje użytkownika i grupy ustalone są zgodnie z normą PN-EN 54-2.

- W sumie można zdefiniować co najmniej 10 różnych kont użytkownika. Logowanie odbywa się przy użyciu numeru seryjnego oraz 8 cyfrowego kodu PIN. W przypadku loginu dla instalatora często bardzo praktyczne jest zdefiniowanie automatycznego odłączania pewnych funkcji np. sygnalizatorów, stałych urządzeń gaśniczych lub urządzeń transmisji alarmu pożarowego.

- Domyślnie centrala jest wyposażona w programowalny przełącznik - zamek z kluczem, który można ustawić w 3 pozycjach. Przy pomocy klucza użytkownik może wykonywać pewnie zaprogramowane wcześniej operacje bez konieczności używania panelu motykowania w celu ich uruchomienia.

- Układ logiczny centrali sygnalizacji pożarowej zawiera automatyczny zegar z kalendarzem oraz co najmniej 19 kanałami. Kanały te można indywidualnie programować jako program dzienny, w którym dla każdego dnia można zaprogramować

10 ustawień użycia jednego z 19 kanałów. Umożliwia to dostosowanie działania systemu np. w dni wolne od pracy. Przy użyciu tych kanałów wyzwolić można konkretne funkcje np.

- o Aktywacja wyjścia
- o Przełączanie w tryb nocny
- o Blokowanie/bypass czujek lub logicznych grup czujek
- o Zmiana poziomu czułości automatycznych czujek pożarowych
- o Zmiana profilu detekcji czujek wielokryteriowych

Potwierdzenie alarmu pożarowego

Przy pomocy panelu dotykowego możliwe jest potwierdzanie alarmu pożarowego wygenerowanego przez automatyczne czujki pożarowe lub ręczne ostrzegacze pożarowe. Praca centrali może być skonfigurowana w dwóch różnych trybach pracy – nocnym i dziennym.

Na panelu dotykowym wyraźnie wyświetlana jest informacja w jakim trybie pracy działa centrala. Przełączanie na tryb dzienny może odbywać się poprzez przekręcenie klucza lub za pomocą panelu dotykowego.

Tryb nocny

Ten tryb pracy przewidziany jest dla sytuacji gdy w obiekcie nie ma obsługi odpowiedzialnej za system sygnalizacji pożarowej. Każdy wykryty alarm pożarowy jest automatycznie przesyłany „na zewnątrz” oraz automatycznie uruchamiana jest sygnalizacja ewakuacji obiektu.

Tryb dzienny

Ten tryb pracy przewidziany jest dla sytuacji gdy w obiekcie przebywa obsługa odpowiedzialna za system sygnalizacji pożarowej. W przypadku wygenerowania alarmu pożarowego uruchamiane jest odliczanie czasu do potwierdzenia przyjęcia alarmu. W tym przedziale czasu osoba odpowiedzialna za system, poinformowana o wystąpieniu alarmu, zobowiązana jest podejść do centrali sygnalizacji pożarowej. Poinformowanie o wystąpieniu alarmu pożarowego musi nastąpić poprzez włączenie brzęczyka w centrali oraz syrenki alarmowej / komunikatu głosowego / systemu pagerowego lub DECT. Przyciskając „Przyjęcie alarmu” na panelu dotykowym, osoba ta potwierdza, że przyjęła informację o alarmie i że uda się zweryfikować prawdziwość alarmu pożarowego. Niezwłocznie po potwierdzeniu przyjęcia alarmu sygnały ostrzegawcze są wyłączane, a użytkownik ma czas na zweryfikowanie alarmu (drugi czas opóźnienia). Jeżeli potwierdzenie alarmu pożarowego nie zostanie dokonane przed upłynięciem czasu na weryfikację centrala sygnalizacji pożaru automatycznie przechodzi w alarmowanie II stopnia, rozpoczyna sygnalizację akustyczną i optyczną alarmu (ewakuacja obiektu) oraz dokonuje niezbędnych wysterowań (np. wysyła informację do straży pożarnej, jeżeli transmisja jest przewidziana).

Czas na weryfikację alarmu jest programowany w zależności od logicznej strefy dozorowej oraz czasu niezbędnego na dotarcie obsługi do danej strefy/czujki.

Pracownik obsługi ma czas na dotarcie do danego miejsca detekcji a następnie na powrót do centrali i albo ręcznie potwierdzić alarm lub zresetować system korzystając z panelu dotykowego. Jeżeli w czasie weryfikacji centrala otrzyma kolejny sygnał alarmu lub wystąpi przerwanie linii dozorowej, automatycznie przejdzie w stan alarmowania II stopnia i rozpocznie sygnalizację akustyczną i optyczną alarmu (ewakuacja obiektu) oraz dokona niezbędnych wystawień (np. wysła informację do straży pożarnej, jeżeli transmisja jest przewidziana).

15.1.7. Redundancja centrali sygnalizacji pożarowej

Zgodnie z normą EN 54, część 2 centrala sygnalizacji pożarowej zawierająca więcej niż 512 elementów LSN, musi zapewniać pełną redundancję kontrolera poprzez użycie drugiego kontrolera jako slave dla kontrolera master aktualnie obsługującego system. W przypadku uszkodzenia kontrolera master, redundantny kontroler slave automatycznie przejmuje wszystkie funkcje systemu zapewniając poprawne działanie systemu na obiekcie. Centrale będą obsługiwały mniej niż 512 elementów.

15.1.8. Zasilacz

Centrala sygnalizacji pożarowej wyposażona jest w wymagane źródło zasilania 24VDC 6A w celu zasilenia szyny modułów, czujek, sygnalizatorów i innego przyłączonego wyposażenia. Zasilacz został zabezpieczony przed przeciążeniem przy pomocy odpowiednich bezpieczników. Zasilanie rezerwowe zapewnione jest poprzez odpowiednie akumulatory o pojemności 40 Ah gwarantujące pełną autonomię systemu w czasie 12/24/72 godzin. Akumulatory są ładowane przez zasilacz w czasie krótszym niż 24 godziny. Moduł zasilania posiada termiczne zabezpieczenie przed przeładowaniem akumulatorów. W celu sprawdzenia poprawności działania akumulatorów wykonywany jest okresowy test. W przypadku gdy wynik tego testu jest negatywny na panelu dotykowym wyświetlany jest komunikat „Uszkodzenie akumulatorów”. W przypadku zaniku zasilania podstawowego system automatycznie i bez zakłóceń przełącza się na zasilanie rezerwowe z akumulatorów. Po 10 minutach wyświetlany jest komunikat „Uszkodzenie zasilania podstawowego”. Moduł baterii akumulatorów wyposażony jest w diody LED w celu sygnalizacji następujących stanów pracy:

- Zasilanie podstawowe OK
- Uszkodzenie/Zanik zasilania podstawowego
- Uszkodzenie akumulatorów

Moduł zasilania akumulatorowego posiada 2 pomocnicze wyjścia 24 VDC do zasilania urządzeń zewnętrznych. Te pomocnicze wyjścia są zabezpieczone automatycznymi bezpiecznikami 2800mA. W przypadku zaniku zasilania podstawowego, wyjścia te są zasilane z akumulatorów.

15.1.9. Moduł liniowy

Moduł liniowy LSN 300 lub równoważny służy do podłączania pętli dozorowej LSN, na której możliwe jest zainstalowanie 254 elementów liniowych z rodziny LSNi (udoskonalona LSN) lub 127 elementów z rodziny klasycznej LSN. Maksymalny pobór prądu w linii to 300 mA.

Maksymalna długość pętli to 1600 m i jest uzależniona od konfiguracji pętli oraz zastosowanego kabla. Istnieje możliwość stosowania kabli nieekranowanych. Maksymalny pobór prądu w linii to 300 mA i jest uzależniony od konfiguracji elementów i typu zastosowanego kabla.

Parametry techniczne:

- a) Napięcie zasilania 20V DC do 30V DC /5V DC \pm 5 %
- b) Napięcie wyjściowe:
 - dla linii dozorowej LSN 30 ± 1.0 V DC
 - jako zasilanie dodatkowe 28 ± 1.0 V DC
- c) Max. pobór prądu 1750 mA przy 24V DC
- d) Nominalny pobór prądu
 - Moduł 39 mA przy 24 V DC
 - Linia dozorowa LSN 1,7 x pobór prądu elementów w linii LSN
 - AUX 1,2 x zasilanie dodatkowe
- e) Maksymalny pobór prądu w linii 300 mA, uzależniony od konfiguracji elementów i typu zastosowanego kabla.
- f) Maksymalny pobór prądu dla zasilania dodatkowego (28 V DC) Max. 500 mA w pętli LSN (system ERT) lub 2 x max. 500 mA w dla dwu linii otwartych
- g) Elementy sygnalizacyjne/obsługi 2 diody LED (czerwona = alarm, żółty = uszkodzenie)
- h) 1 przycisk (sprawdzenie diod LED)
- i) Materiał obudowy ABS, (UL94 V-0)
- j) Dopuszczalny zakres temperatur pracy -5 °C to 50 °C (23 °F to 122 °F)
- k) Dopuszczalny zakres temperatur magazynowania -20 °C to 60 °C (-4 °F to 140 °F)
- l) Dopuszczalna wilgotność względna 95 %, bez kondensacji
- m) Stopień ochrony obudowy zgodnie z normą EN60529 IP 30.

15.1.10. Automatyczne detektory pożaru – czujki punktowe

W celu automatycznego wykrywania spodziewanych pożarów zastosowano dwa typy adresowalnych czujek. Optyczne czujki dymu należy montować w przestrzeni międzysufitowej. Do każdej czujki zamontowanej w przestrzeni międzysufitowej należy podłączyć zewnętrzny wskaźnik zadziałania. Wskaźnik montować na suficie podwieszanym bezpośrednio pod miejscem montażu czujki. Podwójne optyczne czujki dymu montować należy na suficie podwieszanym i na stropie właściwym w przypadku braku sufitu podwieszanego.

15.1.10.1. Optyczne czujki dymu

Automatyczna czujka dymu wyposażona jest w sensor dymu. Posiada inteligentną analizę algorytmu detekcji pożaru z jednakową czułością dla pożarów wytwarzających widzialny dym.

Czujka posiada następujące właściwości:

- automatyczna detekcja dymu dzięki sensorowi optycznemu (światło rozproszone)

- zabezpieczenie przed występowaniem fałszywych alarmów dzięki analizie poziomu i siły sygnału; uzyskane istotne obniżenie podatności na alarmy fałszywe przy utrzymaniu tego samego poziomu wykrywania
- centralnie instalowany optyczny wskaźnik zadziałania w czujce jest widoczny pod każdym kątem, zatem nie jest konieczne ustawianie gniazda czujki względem wejścia do pomieszczenia.
- proste rozwiązanie problemu wadliwego działania poprzez wymianę czujki (cała elektronika w głowicy czujki, gniazdo bez komponentów elektronicznych)
- samokontrola sensorów,
- sygnalizacja uszkodzenia w przypadku uszkodzenia sensora,
- sygnalizacja uszkodzenia w przypadku znacznego zabrudzenia
- automatyczne adresowanie,
- ręczne adresowanie w przypadku stosowania w istniejących sieciach z odgałęzieniami,
- 2 izolatory zwarć (jeden na wejściu drugi na wyjściu z czujki) zostały wbudowane w czujkę w celu zachowania działania innych elementów na pętli LSN nawet w przypadku zwarcia, dlatego nie jest konieczne stosowanie przewodów o wytrzymałości funkcjonalnej.
- kształt czujki oraz labirynt przeciw pyłowy jest tak zaprojektowany, aby umożliwiał swobodne przenikanie dymu do komory optycznej.
- zabezpieczenie przeciw kradzieżowe przeciw nieautoryzowanemu demontażowi czujek z gniazd, który może być opcjonalnie aktywowane
- czujka wysyła sygnał przedalarmowy do CSP w przypadku, gdy osiągnięte zostanie poziom równy 75% ustanowionego progu zadziałania,
- zdalna diagnostyka,
- kompensacja zabrudzenia
- wysoka odporność na zakłócenia elektromagnetyczne zgodnie z umową EFSG/F/97/005
- czujka/gniazdo czujki z zamkiem bagnetowym umożliwiającym wymianę czujki za pomocą teleskopowego uchwytu do wysokości 8 m.
- możliwość podłączenia zdalnego wskaźnika zadziałania,
- przekazywanie informacji o alarmie w formie transmisji danych poprzez dwużyłowy kabel sygnałowy
- wyjście dla wskaźnika zadziałania typu open collector, max. 0V przy 1.5 k Ω
- wskaźnik alarmu: czerwony LED

Parametry elektryczne:

- Napięcie zasilania: 15 V DC.....33 V DC
- Pobór prądu: < 0,55 mA

Parametry mechaniczne:

- Wymiary bez gniazda: Ø 99,5mm x 52mm
- Wymiary z gniazdem: Ø 120mm x 63,5mm

- Materiał obudowy: Plastik, ABS (Novodur)
- Kolor obudowy biały (podobny do RAL 9010) powierzchnia matowa

Parametry środowiskowe:

- Stopień ochrony obudowy zgodnie z EN 60529: IP 40, IP 43 (ze szczelnym gniazdem)
- Dopuszczalny zakres temperatur stosowania: -20 °C . . . +65 °C
- Dopuszczalna wilgotność względna: <95% (bez kondensacji)
- Dopuszczalna prędkość przepływu powietrza: 20 m/s

15.1.10.2. Podwójna optyczna czujka dymu

Automatyczna czujka dymu wyposażona jest w dwa sensory dymu. Posiada inteligentną analizę algorytmu detekcji pożaru z jednakową czułością dla pożarów wytwarzających widzialny dym i wzrost temperatury i wykrywa pożar testowy TF1 zgodnie z EN54.

Czujka posiada następujące właściwości:

- automatyczna detekcja dymu dzięki dwu sensorom optycznym (światło rozproszone) zbudowanym w dwóch diod LED o różnych kolorach/długościach fali (niebieski i podczerwień)
- zabezpieczenie przed występowaniem fałszywych alarmów dzięki analizie poziomu i siły sygnału; uzyskane istotne obniżenie podatności na alarmy fałszywe przy utrzymaniu tego samego poziomu wykrywania
- centralnie instalowany optyczny wskaźnik zadziałania w czujce jest widoczny pod każdym kątem, zatem nie jest konieczne ustawianie gniazda czujki względem wejścia do pomieszczenia.
- proste rozwiązanie problemu wadliwego działania poprzez wymianę czujki (cała elektronika w głowicy czujki, gniazdo bez komponentów elektronicznych)
- samokontrola sensorów,
- sygnalizacja uszkodzenia w przypadku uszkodzenia sensora,
- sygnalizacja uszkodzenia w przypadku znacznego zabrudzenia
- automatyczne adresowanie,
- ręczne adresowanie w przypadku stosowania w istniejących sieciach z odgałęzieniami,
- 2 izolatory zwarć (jeden na wejściu drugi na wyjściu z czujki) zostały wbudowane w czujkę w celu zachowania działania innych elementów na pętli LSN nawet w przypadku zwarcia, dlatego nie jest konieczne stosowanie przewodów o wytrzymałości funkcjonalnej. - kształt czujki oraz labirynt przeciw pyłowy jest tak zaprojektowany, aby umożliwiał swobodne przenikanie dymu do komory optycznej.
- zabezpieczenie przeciw kradzieżowe przeciw nieautoryzowanemu demontażowi czujek z gniazd, który może być opcjonalnie aktywowane
- czujka wysyła sygnał przedalarmowy do CSP w przypadku, gdy osiągnięte zostanie poziom równy 75% ustanowionego progu zadziałania,
- zdalna diagnostyka,

- kompensacja zabrudzenia,
- wysoka odporność na zakłócenia elektromagnetyczne zgodnie z umową EFSG/F/97/005,
- czujka/gniazdo czujki z zamkiem bagietowym umożliwiającym wymianę czujki za pomocą teleskopowego uchwyty do wysokości 8 m.,
- możliwość podłączenia zdalnego wskaźnika zadziałania,
- przekazywanie informacji o alarmie w formie transmisji danych poprzez dwużyłowy kabel sygnałowy,
- wyjście dla wskaźnika zadziałania typu open collector, max. 0V przy 1.5 k Ω
- wskaźnik alarmu: czerwony LED.
- Parametry elektryczne:
- Napięcie zasilania: 15 V DC.....33 V DC,
- Pobór prądu: < 0,55 mA.

Parametry mechaniczne:

- Wymiary bez gniazda: Ø 99,5mm x 52mm
- Wymiary z gniazdem: Ø 120mm x 63,5mm
- Materiał obudowy: Plastik, ABS (Novodur)
- Kolor obudowy biały (podobny do RAL 9010) powierzchnia matowa

Parametry środowiskowe:

- Stopień ochrony obudowy zgodnie z EN 60529: IP 40, IP 43 (ze szczelnym gniazdem)
- Dopuszczalny zakres temperatur stosowania: -20 °C . . . +65 °C
- Dopuszczalna wilgotność względna: <95% (bez kondensacji)
- Dopuszczalna prędkość przepływu powietrza: 20 m/s

15.1.11. Ręczny ostrzegacz pożaru

System zostanie wyposażony w czujki ręczne zwane Ręcznymi Ostrzegaczami Pożarowymi (ROP). Ręczne ostrzegacze pożarowe powinny być instalowane w widocznych i łatwo dostępnych miejscach wzdłuż dróg ewakuacyjnych.

- Ostrzegacz należy instalować na wysokości 140cm (\pm 20cm), mierzonej od środka ostrzegacza do podłogi.

Zaprojektowany ROP jest urządzeniem adresowalnym, montowany natynkowo o bezpośrednim działaniu, kasowalny, do zastosowania wewnątrz obiektów, koloru czerwonego.

Podstawowe właściwości:

- Zgodny z wymaganiami normy EN 54-11, posiada certyfikat CPD,
- uruchamianie alarmu pożarowego poprzez wciśnięcie czarnego znaku,
- zabezpieczony przed skałeczeniem, nie ma szybki,
- sygnalizacja zadziałania na czerwono na panelu przednim,
- sygnalizacja zadziałania LED do celów sprawdzenia,

- nadzorowane połączenie z CSP,
- indywidualna identyfikacja ROP polegająca na wyświetlaniu adresu w celu szybkiej identyfikacji miejsca uruchomienia,
- samomonitorowanie: Uszkodzenie jest sygnalizowane w CSP łącznie z podaniem adresu ROP, co umożliwia szybką lokalizację w obiekcie,
- ręczne adresowanie w przypadku stosowania w istniejących systemach z liniami otwartymi,
- 2 zintegrowane izolatory zwarć (jeden na wejściu drugi na wyjściu z urządzenia) umożliwiające pełną funkcjonalność pozostałych elementów pętli w dozorowej LSN, nawet przypadku przerwy lub zwarcia obwodu. Nie jest zatem wymagane stosowanie kabli o podwyższonej wytrzymałości. Izolatory spełniają wymagania normy EN 54-17,
- możliwość stosowania kabli nieekranowanych,
- otwieranie, sprawdzanie, resetowanie ROP jednym kluczem,
- pod przezroczystą klapką można umieścić dodatkowe oznakowanie,
- możliwość dodania następujących akcesoriów:
 - przezroczysta klapka na zawiasach, do zabezpieczania przed przypadkowym uruchomieniem ROP,
 - uszczelnienie dodatkowej klapki.

Parametry techniczne

- Napięcie zasilania: 15 V DC...33 V DC,
- Pobór prądu: < 0.4 mA,
- Stopień ochrony obudowy EN 60529: Min. IP 52,
- Obudowa: - materiał plastik, ABS (Novodur), kolor czerwony lub podobny do RAL 3001,
- Dopuszczalna temperatura pracy: -25 °C . . . +70 °C.

15.1.12. Wskaźnik zadziałania

Wskaźnik zadziałania sygnalizuje stan alarmowy czujki umieszczonej w przestrzeni sufitu podwieszonego. Wskaźniki umieszczone zostaną na suficie podwieszonym pod czujką.

Dane techniczne

- | | | |
|------------------------------|---|---|
| • Napięcie zasilania | - | 9 VDC . . . 30VDC |
| • Pobór prądu przez wskaźnik | - | T.2 ok. 2 mA, T.3 ograniczenie do ok. 13 mA,
T.4 ograniczenie do maks. 20 mA |
| • wskazanie zadziałania | - | 1 dioda LED przez trzpień światłowodowy |
| • Dopuszczalna grubość żyły | - | 0,6 - 0,8 mm |
| • Klasa ochrony zgodnie z | - | IEC 60529, IP 40 |

15.1.13. Moduł sterujący 8 wejść, 1 wyjście – typ 1

W systemie, na „pętlach sterujących”, należy zainstalować moduły sterujące z 8 nadzorowanymi wejściami i jednym wyjściem przekaźnikowym.

Właściwości:

- 8 nadzorowanych wejść i jedno wyjście przekaźnikowe,
- możliwość wyboru pomiędzy nadzorowaniem styków z wykorzystaniem rezystora końca linii (rezystor EOL) lub bez nadzorowania (bez rezystora EOL),
- wejścia programowalne, w przypadku aktywacji wejścia styk się zamyka lub otwiera
- sposób nadzorowania funkcji wybierany niezależnie dla każdego wejścia,
- przekaźnik do przełączania prądów i napięć do 2 A/30 V DC,
- dostarczany z obudową do montażu natynkowego,
- zaciski wtykane umożliwiają prosty sposób instalacji okablowania i konserwacji urządzeń,
- zaciski śrubowe umożliwiają podłączanie przewodów o maksymalnej średnicy 3,3 mm²,
- dostęp serwisowy do zacisków jest możliwy bez konieczności zdejmowania obudowy,
- może być włączany do dozorowych pętli, linii otwartych i bocznych,
- dwa wbudowane izolatory zwarć zgodne z EN 54-17,
- zasilanie modułu z linii dozorowej 2 żyłowej (nie wymaga zasilania dodatkowego),
- adresowanie automatyczne lub poprzez przełącznik kodujący (umożliwia jednoznaczne przypisanie lokalizacji w obiekcie do adresu),
- możliwość stosowania kabli nieekranowanych,
- zgodny z normą EN 54-18 (moduły wejścia/wyjścia).

Parametry techniczne

- Maksymalna obciążalność wyjścia: 2,0 A przy 30 V DC,
- Maksymalny pobór prądu: 5,5 mA,
- Stopień ochrony IP 43 zgodnie z normą EN 60529,
- Obudowa modułu: mieszanka ABS + PC, kolor biel sygnałowa, zbliżony do RAL 9003,
- Dopuszczalny zakres temperatur pracy: -20 °C . . . +65 °C,
- Dopuszczalna wilgotność względna: < 96%.

15.1.14. Moduł sterujący 8 wyjść – typ 2

W systemie, na „pętlach sterujących”, należy zainstalować moduły sterujące z 8 wyjściami przekaźnikowymi.

Właściwości:

- Osiem przekaźników ze stykiem przełącznym – bezpotencjałowe styki wyjściowe,
- Maksymalne obciążenie styków 2A / 30VDC,
- Adres elementu ustawiany za pomocą przełączników obrotowych,
- Wbudowany izolator,

Parametry techniczne

- Napięcie wejściowe sieci LSN - 15 VDC - 33 VDC (min. – maks.)
- Maks. pobór prądu z sieci LSN - 3,55 mA
- 8 przekaźników
- (niskonapięciowych) - (styk NC / COM / styk NO)
- Obciążalność styków
(obciążenie rezystancyjne):

Maks. prąd przełączania	-	2 A
Maks. napięcie przełączania	-	30VDC
Min. prąd przełączania	-	0,01 mA
Min. napięcie przełączania	-	10 mVDC
- Połączenia - Zaciski śrubowe
- Średnica żyły - 0,6 - 3,3 mm²
- Ustawienia adresów - 3 przełączniki obrotowe
- Materiał - ABS + PC-FR
- Wymiary - ok. 140 x 200 x 48 mm (szer. x wys. x gł.)
- Masa (bez / z opakowaniem) - ok. 490 g / 810 g
- Temperatura pracy - -20°C ÷ 65°C
- Temperatura przechowywania - -25°C ÷ 80°C
- Dopuszczalna wilgotność względna - < 96% (bez kondensacji)
- Klasa wyposażenia zgodnie z IEC 60950 - Urządzenie stopnia III
- Stopień ochrony zgodnie z IEC 60529 - IP 54

15.1.15. Okablowanie dla systemu ppoż

System sygnalizacji pożarowej stanowi niezależną wydzieloną instalację bezpieczeństwa, w związku z czym nie może być wspólny z siecią innej instalacji.

W przypadku montażu czujek na stropie właściwym gdzie występuje sufit stały nierozbieralny (płyty G-K) należy zapewnić rewizje serwisowe.

Wytyczne:

- połączenia między elementami systemu sygnalizacji pożarowej wykonać zgodnie z projektem i wytycznymi zawartymi w części opisowej,
- zastosowane kable w liniach dozorowych i sterowniczych powinny posiadać izolację zewnętrzną w kolorze czerwonym,
- uszkodzenie w sieci kablowej powinno być sygnalizowane w centrali CSP,
- linie do wskaźników zadziałania należy wykonać nieekranowanym kablem typu YnTKSY 1x2x1mm (kolor czerwony),
- linie monitorowania i sterowania urządzeń niewymagających zasilania w czasie pożaru lub pracujących przy otwarciu obwodów układów sterujących należy

wykonać kablem telekomunikacyjnym nieekranowanym typu YnTKSY 1x2x0,8mm tzn. monitorowane położenia klap pożarowych odcinających, sterowanie i monitorowanie central oddymiania,

- Dla czujek punktowych przewody YnTKSY 1x2x0,8mm (wewnętrzna pętla pożarowa). Przewody należy układać w osobnych, niezależnych trasach tworzących pętle,
- Pętla prowadzona na zewnątrz przewody typu XzKAXw 3x2x0,8mm, przejścia dokonać w puszkach certyfikowanych,
- Dla sterowań 24VDC wymagających działania podczas pożaru przewody niepalne np. (N)HXH PH90 2x1,5mm² tworzące zespół kablowy,
- Dla podania styku wyłączającego działanie central wentylacyjnych - przewody niepalne np. (N)HXH PH90 2x1,5mm² tworzące zespół kablowy,
- okablowanie bez odporności ogniowej (odporność ogniowa PH0) np. pętli dozorowych należy prowadzić w np. na uchwytach mocowanych bezpośrednio do stropu stałego, rurkach RL w przestrzeni między sufitowej. W pomieszczeniach biurowych podtynkowo.
- okablowanie o odporności ogniowej prowadzić zgodnie z wymaganiami producenta tych kabli oraz obowiązującymi normami i przepisami, koryta kablowe o odporności ogniowej ma tworzyć zespół kablowy.
- należy unikać prowadzenia linii systemu sygnalizacji pożaru w pobliżu innych instalacji elektrycznych oraz zachować odległości koordynacyjne przy zbliżeniach.

15.1.16. Zasilanie podstawowe i awaryjne

W systemie należy przewidzieć zasilanie podstawowe z wydzielonego obwodu zasilania z rozdzielni pożarowej (wg opracowania części elektrycznej):

- 1) central CSP,
- 2) zasilaczy ppoż.

Zestawienia bilansów:

Dobierając wielkość baterii akumulatorów rezerwowych dla central należy kierować się zasadą, iż jej pojemność, w przypadku zaniku napięcia sieci, powinna wystarczyć przynajmniej na:

1. 4 h pracy systemu w stanie dozorowania, w przypadku, gdy służby serwisowe są stale dostępne i dysponują odpowiednim wyposażeniem, umożliwiającym szybkie usunięcie awarii;
2. 30 h pracy systemu w stanie dozorowania, w przypadku, gdy zapewniona jest możliwość naprawy awarii zasilania przez służby serwisowe w ciągu 24 h (np. w wyniku zawarcia odpowiedniej umowy z firmą prowadzącą konserwację instalacji)
3. 72 h pracy systemu w stanie dozorowania, w przypadku, gdy powyższe warunki nie są spełnione.

Dodatkowo w obliczeniach należy uwzględnić wymaganą 0,5 h pracę systemu w stanie alarmowania. Dla precyzyjnego obliczenia pojemności baterii akumulatorów

rezerwowych można posłużyć się wzorem:

$$QAh = \frac{I_{doz} \cdot T_{doz} + I_{al} \cdot T_{al}}{1,25}$$

, gdzie:

- QAh wymagana pojemność akumulatorów w Ah
1,25 współczynnik zwiększenie pojemności akumulatorów o 25%
 na skutek ewentualnych strat ich pojemności w wyniku starzenia
 I_{doz} pobór prądu przez instalację w stanie dozoru w A
 T_{doz} wymagany czas pracy systemu, równy 4 h, 30 h lub 72 h
 I_{al} pobór prądu podczas alarmowania w A
 T_{al} wymagany czas alarmowania, równy 0,5 h

15.1.17. Współpraca z innymi systemami

Centrala sygnalizacji pożarowej steruje urządzeniami automatyki pożarowej za pośrednictwem modułów sterujących zainstalowanych na pętlach dozoru w bezpośrednim sąsiedztwie sterowanych urządzeń. Moduły wyposażone są w przekaźnik bistabilny, który w zależności od sposobu podłączenia okablowania może mieć postać NC lub NO.

15.1.18. Wytyczne w zakresie przeglądów i konserwacji

System ppoż. należy regularnie poddawać okresowym przeglądom konserwacyjnym zgodnie z przepisami wytycznymi i zaleceniami producenta. Kontrole okresowe powinny być przeprowadzane zgodnie z PKN-CEN/TS 54-14:2006 przez uprawnionego instalatora, w zakresie kontroli, obsługi technicznej i naprawy. Nazwa i numer telefonu Konserwatora powinny być wyraźnie uwidocznione przy CSP.

Umowy w tym zakresie powinny być zawarte po zakończeniu montażu, niezależnie od tego, czy obiekt jest użytkowany, czy też nie.

16. System BMS

System BMS obejmuje dostawę, montaż, regulację, zaprogramowanie, oraz rozruch wykonanego systemu do monitoringu i / lub sterowania instalacji podanych w niniejszym opisie.

System BMS został zaprojektowany jako centralny system komputerowy oparty o serwer i stację roboczą oraz sterowniki połączone ze sobą strukturą sieci komunikacyjnych. Podstawowym celem systemu jest zapewnienie sterowania i/lub monitorowania instalacji do niego podłączonych. Projektuje się system oparty o otwarte sieci komunikacyjne, dzięki czemu system będzie przystosowany do ewentualnej rozbudowy w przyszłości o dodatkowe urządzenia spełniające standard tych komunikacji.

Inwestycja podzielona została na dwa główne etapy: etap 1B oraz etap 2. W etapie 1B zakłada się dostawę, montaż, regulację, zaprogramowanie, oraz rozruch instalacji BMS służących do monitorowania i sterowania instalacji rozmieszczonej w obszarze etapu 1B. Wiąże się to także z wizualizacją ich w centralnym stanowisku nadzoru. W etapie 2 BMS obejmuje zatem dostawę, montaż, regulację, zaprogramowanie, oraz rozruch instalacji BMS służącej do monitoringu i/lub sterowania dobudowanych instalacji.

Wiąże się to także ze zmianami programu w sterownikach zamontowanych w etapie 1b w zakresie monitoringu i sterowania instalacjami dołożonymi w etapie 2 oraz z dołożeniem wizualizacji tych instalacji w centralnym stanowisku nadzoru.

16.1. Komponenty systemu BMS

Projektuje się system BMS oparty o następujące komponenty:

- Centralne stanowisko nadzoru:
 - Serwer systemu BMS
 - Oprogramowanie nadzorcze
 - Stacja operatorska
- Sterowniki BMS:
 - Sterowniki swobodnie programowalne
 - Moduły rozszerzeń wejść/wyjść sterownika
 - Moduły komunikacyjne integrujące system z sieciami komunikacyjnymi
- Rozdzielnice BMS
- Sieci komunikacyjne Ethernetowe
- Sieci komunikacyjne szeregowe
- Trasy kablowe.

16.2. Centralne stanowisko nadzoru

Centralne stanowisko nadzoru oparte będzie o serwer z zainstalowanym oprogramowaniem nadzorczym. Jako interfejs użytkownika służyć będzie stacja operatorska. Oprogramowanie nadzorcze zostanie zainstalowane na serwerze przez wykonawcę systemu. Wykonawca opracuje także kolorowe strony graficzne wizualizując systemy dołączone do BMSa. Dane będą prezentowane w postaci kolorowych aktywnych grafik, animacji, tekstu oraz wykresów. Wszystkie kolorowe strony będą tworzyły logiczną całość oraz będą wykonane estetycznie. Nawigacja pomiędzy stronami odbywać się będzie za pomocą odnośników. Alarmy będą raportowane oraz wizualizowane w widoczny sposób (np. przez podkreślenie lub zmianę koloru grafiki). Dane historyczne będą gromadzone w bazach programu nadzorczego. Operator będzie miał możliwość zmiany parametrów danych z poziomu stacji operatorskiej. Dostęp do poszczególnych parametrów (nastawników, przycisków, ikon, wartości itp.) będzie możliwy w zależności od poziomu użytkownika (hierarchii użytkownika wraz z jego przywilejami). Wszystkie dane wyświetlane na grafice będą odświeżane dynamicznie.

Serwer będzie zlokalizowany w serwerowni w obszarze Hali.

Minimalne wymagania serwera BMS oraz stacji operatorskiej:

- Procesor: Intel Pentium™ IV, 2 GHz lub wyższy
- System operacyjny:
 - Windows Server 2012 Standard/Enterprise (SP2, 64-bit) (R2)
 - Windows 7 Professional/Enterprise/Ultimate (32-bit lub 64 bit)
 - Windows 8 Professional/Enterprise/Ultimate (32-bit lub 64 bit)

- Windows 8.1 Professional/Enterprise/Ultimate (64-bit)
 - Windows 10 (64-bit)
- Dysk twardy: min. 500GB
- Pamięć RAM: 4 GB dla systemów 32-bit, 8 GB dla systemów 64 bit
- Karta graficzna
- Karta sieciowa: 2 x karta 1 x Gigabit LAN RJ-45
- Porty: 4 x USB
- Port typu COM
- Napęd optyczny: Nagrywarka DVD
- Zainstalowana przeglądarka internetowa Internet Explorer 8.0 lub wyższa
- Stacja operatorska dodatkowo wyposażona w:
 - Monitor: LCD 24"
 - Mysz: optyczna
 - Klawiatura

Komputery zostaną dostarczone wraz ze wszystkimi wymaganymi licencjami. Serwer oraz stacja nadzorcza będą dostosowane do pracy ciągłej, tj. przez 24 godziny 7 dni w tygodniu.

16.3. Sterowniki BMS

Projektuje się system BMS w oparciu o sterowniki swobodnie programowalne typu PLC wykonane w standardzie przemysłowym, ale dedykowane do instalacji budynkowych. Jednostki główne sterowników komunikują się ze sobą przy użyciu komunikacji z protokołem BACNet IP. Do jednostek głównych dołączone będą moduły komunikacyjne oraz moduły wejść/wyjść. Sterowniki zabudowane zostaną w rozdzielnicach BMS. Dopuszcza się, aby moduły wejść/wyjść zdalne były montowane w rozdzielnicach elektrycznych po wcześniejszych ustaleniach z branżą elektryczną. Każdy z zaprojektowanych sterowników BMS będzie posiadać następujące funkcje:

- Każdy sterownik BMS będzie posiadał własny webserwer
- Każdy sterownik BMS jest sterownikiem swobodnie programowalnym
- Każdy sterownik BMS posiadać będzie zegar czasu rzeczywistego
- Aplikacja sterownika zawiera swobodnie definiowane zależności programowe
- Każdy sterownik BMS będzie posiadał możliwość zastosowania sterowania procesami w funkcji terminarza z wykorzystaniem mechanizmu Optymalnego Startu Stopu
- Istnieje możliwość zmiany głównego protokołu komunikacyjnego bez potrzeby wymiany całego sterownika
- Istnieje możliwość dodania dodatkowego protokołu do sterownika poprzez moduł komunikacyjny
- Sterowniki będą pełniły indywidualne funkcje i są zaprojektowane jako odrębnie działające jednostki. Oznacza to, że rozłączenie któregośkolwiek sterownika

BMS od centralnego systemu nadzoru spowoduje, że sterownik ten będzie działał nadal na parametrach ostatnio zapamiętanych.

Układy monitorowane lub sterowane będą łączone przy użyciu protokołów komunikacyjnych lub wejść/wyjść cyfrowych/analogowych. Peryferyjne protokoły takie jak MODBUS TCP, MODBUS RTU, M-BUS i inne otwarte będą połączone ze sterownikami BMS przy użyciu dedykowanych modułów komunikacyjnych zabudowanych w sterowniku bądź dokładanych do niego jako moduł pomocniczy. Układy monitorowane i/lub sterowane przy użyciu sygnałów cyfrowych i analogowych będą połączone ze sterownikiem poprzez wejścia/wyjścia zabudowane w jednostce głównej bądź w module pomocniczym wejść/wyjść.

16.4. Rozdzielnice BMS

W rozdzielnicach BMS będą zabudowane sterowniki systemu BMS. Wszystkie rozdzielnice BMS powinny spełniać następujące kryteria:

- Powinny być wyposażone w komplet aparatury niezbędnej do monitorowania i sterowania poszczególnych instalacji
- Rozdzielnice BMS wraz z wyposażeniem powinny spełniać obowiązujące przepisy oraz normy dotyczące rozdzielnic sterowniczych
- Obudowy powinny być trwałe i zapewniające odpowiednie IP zależne środowiska w którym zostaną zamontowane
- Wyłączniki główne rozdzielnic powinny być zamontowane z przodu lub z boku obudowy
- Części wewnętrzne rozdzielnic BMS, które zostają pod napięciem po odłączeniu wyłącznika głównego winny być odpowiednio oznakowane.
- Wszystkie elementy rozdzielnic BMS muszą być oznakowane zgodnie ze schematami warsztatowymi
- Każda z rozdzielnic BMS będzie posiadała wewnątrz schemat połączeń elektrycznych
- Wszystkie szafy BMS powinny być oznakowane zgodnie z projektem w sposób przejrzysty i jednoznaczny
- Oznaczenia na rozdzielnicach powinny być widoczne i zawierać nazwę rozdzielnic oraz informację „Pod napięciem”.

16.5. Funkcjonalność systemu BMS

Projektuje się system BMS monitorujący i/lub sterujący instalacją elektryki w zakresie: kontroli zasobów energetycznych budynku, kontroli zużycia energii elektrycznej przez najemców, systemu SZR, sterowania oświetlenia komunikacji i toalet, sterowania oświetlenia trybun i płyty boiska, sterowania iluminacją budynku.

16.6. Kontrola układów SZR

Układy samoczynnego załączenia rezerwy SZR działają w dwóch częściach instalacji elektrycznej. Pierwszy układ (SZR1) umieszczony zostanie w rozdzielnic SN, natomiast drugi (SZR2) umieszczony zostanie w rozdzielnic głównej NN

(RGSN). Należy przystosować system BMS do czytywania sygnałów z SZRów. Rodzaj komunikacji zostanie uzgodniony na etapie wykonawstwa z branżą elektryczną. Dopuszcza się stosowanie zarówno sygnałów cyfrowych jak i komunikacji po protokole otwartym.

16.7. Kontrola zasobów energetycznych budynku

W rozdzielnicy NN budynku (RGNS) zostaną zamontowane mierniki parametrów sieci niskiego napięcia. Mierniki te zostaną wyposażone w komunikację szeregową po protokole MODBUS RTU. System BMS będzie monitorował parametry takie jak: napięcie, natężenie prądu, zużycie energii elektrycznej, częstotliwość, współczynnik mocy.

16.8. Monitoring zużycia energii elektrycznej

Liczniki energii elektrycznych zostaną zabudowane w rozdzielnicach SN i/lub NN. Opomiarowane zostaną poszczególne części budynku jak i pomieszczenia przeznaczone do wynajmu. Liczniki po stronie średniego napięcia będą wyposażone w bramki komunikacyjne przekształcające sygnał z liczników na sygnał Ethernetowy. Pozostałe liczniki będą miały możliwość podłączenia się po komunikacji szeregowej M-BUS. System BMS monitorować będzie zużycie energii elektrycznej zmierzonej przez te liczniki.

16.9. Sterowanie oświetleniem

Zasilanie obwodów oświetleniowych zaprojektowanych do starowania przez BMS zostanie wykonane przez styczniki, tak, aby można było sterować nimi przy użyciu sygnałów cyfrowych. W systemie BMS projektuje się sterowanie oświetleniem w zakresie:

- Oświetlenie obszarów wspólnych (rozdzielnice RO)
- Iluminacja budynku (rozdzielnice RO)
- Oświetlenie płyty głównej boiska (rozdzielnice ROB)
- Oświetlenie trybun (rozdzielnice ROB)

Sterowanie podzielone będzie na sekcje i odbywać się będzie według wytycznych branży elektrycznej.

16.10. Monitoring UPS

W celu zapewnienia zasilania bezprzerwowego wybranych instalacji zostały zaprojektowane zasilacze UPS. Wyposażone zostaną w karty komunikacyjne MODBUS RTU. Projektuje się system BMS umożliwiający monitoring tych sygnałów.

16.11. Monitoring rozdzielnic elektrycznych

Rozłączniki zamontowane w rozdzielnicy głównej NN (RGNS) posiadać będą styki pomocnicze sygnalizujące przepalenie ich wkładek. Każda istotna rozdzielnica elektryczna będzie posiadać styki bezpotencjałowe sygnalizujące pozycję ich wyłączników głównych. Poza tym każdy z ochronników przeciwprzepięciowych także

będzie wyposażony w styk bezpotencjałowy sygnalizujący przepalenie ochronnika. Wszystkie te sygnały będą monitorowane przez system BMS poprzez wejścia cyfrowe na sterownikach i modułach wejść/wyjść.

17. Dane techniczne obiektu charakteryzujące wpływ na środowisko

17.1. Oddziaływanie i emisja szkodliwych czynników

Projektowana instalacja i zasilane urządzenia nie wpływają negatywnie na środowisko. Występowania wyższych harmonicznych od dopuszczalnych nie przewiduje się. Występowania pól elektromagnetycznych, wibracji i drgań pochodzenia energetycznego nie przewiduje się.

17.2. Wpływ obiektu na drzewostan i glebę

Projektowana instalacja nie wpływa na stan drzewostanu i wody powierzchniowe i podziemne.

18. Warunki ochrony przeciwpożarowej

Wszystkie przejścia przez strefy pożarowe uszczelnić masami do klasy przegrody. Uszczelnienia biernej ochrony pożarowej należy dobrać wg oferty firm np. PROMAT, HILTI.

Wszystkie zaprojektowane przewody posiadają zdolność pracy w przewidzianych warunkach przez czas zgodny z Normą Polską.

19. Uwagi końcowe

1. Wszystkie wykonywane prace oraz materiały winny odpowiadać Polskim Normom i posiadać stosowną deklarację zgodności lub posiadać znak CE i deklarację zgodności z normami zharmonizowanymi oraz posiadać niezbędne atesty i certyfikaty tak aby spełniać obowiązujące przepisy.
2. Po zakończeniu robót wykonać pomiary skuteczności ochrony od porażeń prądem elektrycznym i sporządzić protokół,
3. Należy stosować urządzenia z certyfikatami zezwalającymi na ich stosowanie i użytkowanie w ochronie przeciwpożarowej oraz budownictwie na terenie RP.
4. Trasowanie przewodów elektrycznych należy wykonać uwzględniając konstrukcję budynku oraz zapewniając bezkolizyjność z innymi instalacjami. Trasa instalacji winna być przejrzysta, prosta i dostępna do prawidłowej konserwacji i remontów. Wskazane jest, aby w miarę możliwości trasa przebiegała w liniach pionowych i poziomych. Przy trasowaniu ciągów instalacji należy dążyć do jak najmniejszej liczby skrzyżowań i zbliżeń z ciągami instalacji elektromagnetycznych i innymi instalacjami.
5. Szerokość bruzd pod wszystkie przewody elektryczne należy dostosować do średnicy przewodu z uwzględnieniem rodzaju i grubości tynku. Przewody należy układać

jednowarstwowo. Zabrania się kucia bruzd w elementach konstrukcyjnych oraz w cienkich ścianach działowych.

6. Po wykonaniu robót montażowych należy sprawdzić ciągłość żył i powłok instalacyjnych oraz zgodność faz, dokonać pomiaru rezystencji izolacji i wykonać próbę napięciową.
7. Badanie rezystancji izolacji instalacji elektrycznej powinno być zakończone protokołem i zawierać: miejsce wykonania pomiarów, datę wykonania, datę ważności pomiarów oraz rodzaj, typ i numer miernika, zakres pomiarów, napięcie pomiarowe, wyniki pomiarów poddane analizie, ocenę stanu instalacji oraz informacje, które według Wykonawcy mogą mieć znaczenie w ocenie stanu faktycznego.
8. Zapewnić stałą obsługę konserwacyjną i przegląd systemu.
9. Użytkować system zgodnie z zaleceniami producenta ujętymi w instrukcji użytkowania i podczas szkolenia po zainstalowaniu systemu.
10. Prace powinny być wykonywane zgodnie z dokumentacją projektową.
11. Przy wyznaczaniu ciągów instalacyjnych należy dążyć do jak najmniejszej liczby skrzyżowań z innymi instalacjami. Wskazane jest zachowanie odległości min 10 cm.
12. Przy prowadzeniu instalacji równoległe z instalacją elektryczną przewody instalacji sygnalizacji pożaru powinny przebiegać poniżej.
13. Przewody między elementami systemu nie mogą być przedłużane – muszą to być przewody jednoodcinkowe.
14. Czujki chroniące przestrzeń międzystropową montować na stropie rzeczywistym. Od każdej czujki chroniącej przestrzeń międzystropową wyprowadzić na sufit podwieszany wskaźnik zadziałania czujki.
15. W przypadku, gdy sufit podwieszany nie jest rozbieralny należy wykonać otwory rewizyjne o wymiarach 60x60cm pod każdą czujką zamontowaną w przestrzeni międzystropowej.
16. Odstępy czujek punktowych od ścian nie mogą być mniejsze niż 50cm. Minimalna odległość czujek od kratek nawiewnych i wywiewnych wynosi 1,5m.
17. W przypadku, kiedy układ kratek wentylacyjnych uniemożliwia zamontowanie czujki w środku geometrycznym należy sprawdzić czy nie zostanie przekroczona maksymalna odległość pozioma pomiędzy czujką ścianą.
18. W pomieszczeniu z centralką SAP umieścić zafoliowany plan sytuacyjny dozorowanego przez system obiektu z zaznaczeniem na nim wszystkich elementów adresowalnych z czytelnymi numerami logicznymi wchodzącymi w skład systemu.

19. Wykonawca oznaczy numerami logicznymi czytelnymi z poziomu podłogi wszystkie zamontowane elementy (czujki, przyciski ROP, wskaźniki zadziałania, moduły sterujące)
20. Matryca sterowań oraz lista sterowań powinna być uzgodniona każdorazowo dla każdego obiektu z rzeczoznawcą pożarowym i kierownikiem ds. Bezpieczeństwa Inwestora.

Przepisy BHP

Prace instalacyjne oraz inne muszą być wykonane zgodnie z obowiązującymi przepisami bhp dla wszystkich branż.

Uwagi ogólne

Wszelkie zmiany dokonywane w obiekcie mogące mieć wpływ na efektywność systemu, muszą być uzgadniane projektantem / wykonawcą systemu.