Spis rysunków

Podstawa projektowania

Wytyczne użytkownika, uzgodnienia z użytkownikiem, projekt architektoniczny oraz projekty branżowe (instalacji elektrycznych, sanitarnych, konstrukcji, organizacji ruchu).
Akty prawne:

- Prawo Budowlane. (Dz.U. 1995 nr 89, poz. 414) wraz z późniejszymi zmianami,
- Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r., w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie wraz z późniejszymi zmianami.
- Rozporządzenie Ministra Spraw Wewnętrznych z dnia 3 listopada 1992 r., w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów. (Dz. U. 1992 nr 92, poz. 460)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 listopada 1998r, w sprawie szczegółowego zakresu i formy projektu budowlanego. (Dz. U. 1998 nr 140, poz. 906)
- Dz. U. z 2003r., Nr 121, Poz. 1136 i 1137 Rozporządzenie Ministra Spraw Wewnętrznych I Administracji z dnia 16 czerwca 2003 r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej
- Dz. U. 2004r., Nr 195, Poz. 2011 Rozporządzenie Ministra Infrastruktury z dnia 11 sierpnia 2004 r. w sprawie systemów oceny zgodności, wymagań, jakie powinny spełniać notyfikowane jednostki uczestniczące w ocenie zgodności, oraz sposobu oznaczania wyrobów budowlanych oznakowaniem CE
- Dz. U. z 2007 r., Nr 143, poz. 1002 Rozporządzenie Ministra Spraw Wewnętrznych I Administracji z dnia 20 czerwca 2007 r. w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania
- Dz. U. z 2010 r. Nr 85, poz. 553 Rozporządzenie Ministra Spraw Wewnętrznych. i Administracji z dnia 27 kwietnia 2010 r. zmieniające rozporządzenie w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronią zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania.
- PKN-CEN/TS 54-14:2006 Systemy sygnalizacji pożarowej. Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji.
- Polska Norma PN-EN 60849 – Dźwiękowe systemy ostrzegawcze.
- PN-EN 54-4: Systemy sygnalizacji pożarowej – Część 4: Zasilacze.

- PN-EN 54-16: Systemy sygnalizacji pożarowej – Część 16: Centrale dźwiękowych systemów ostrzegawczych.
- PN-EN 54-24 Systemy sygnalizacji pożarowej – Część 24: Dźwiękowe systemy ostrzegawcze – Głośniki.
- Norma Brytyjska BS 5839-8 -Dźwiękowe systemy ostrzegawcze.
- PN-EN 12101-6:2007 Systemy kontroli rozprzestrzeniania się dymu i ciepła. Część 6: Wymagania techniczne dotyczące systemów różnicowania ciśnień.
- PN-IEC 60364-1:2000 Instalacje elektryczne w obiektach budowlanych. Zakres, przedmiot i wymagania podstawowe.
- PN-IEC 60364-3:2000 Instalacje elektryczne w obiektach budowlanych. Ustalanie ogólnych charakterystyk.
- PN-IEC 60364-5-52:2002 - Instalacje elektryczne w obiektach budowlanych. Dobór i montaż wyposażenia elektrycznego. Oprzewodowanie.
- PN-IEC 664-1:1998 Koordynacja izolacji urządzeń elektrycznych w układach niskiego napięcia. Zasady, wymagania, badania.
- PN-EN 50173-1:2004 oraz ISO/IEC 11801:2002 podstawowe zalecenia dotyczące instalowania okablowania ekranowanego i nieekranowanego.
- PN-EN 50174-1:2002 „Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości.”
- PN-EN 50174-2:2002 „Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków”.
- PN-EN 50346:2002 „Technika informatyczna. Instalacja okablowania. Badanie zainstalowanego okablowania”
- Norma ANSI/TIA/EIA 568B.2-1: June 2002 Commercial Building Telecommunications Wiring Standard
- PN-EN 50310:2002 „Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym”
- ISO/IEC 11801 Technika informatyczna. Systemy okablowania strukturalnego.
- PN-EN 50173 (europejski odpowiednik normy ISO/IEC 11801)
- Norma EIA/TIA-568A (amerykański odpowiednik międzynarodowej normy ISO/IEC 11801)
- BN-84/8984-10 Telekomunikacyjne sieci miejscowe. Instalacje wnętrzowe. Wymagania ogólne.
- PN-74/8984.05 Elektroenergetyczne i sygnalizacyjne linie kablowe. Projektowanie i budowa.

- EN 50132-7:1996 +AC:1997 E Systemy alarmowe. Systemy dozorowe CCTV w zastosowaniach dotyczących zabezpieczeń.
- PN-E-08390-1 :1996 Systemy alarmowe – Terminologia
- PN-EN 50130-5 :2002 Systemy alarmowe – Część 5 Próby środowiskowe
- PN-93/E-08390/12 :1993 Systemy alarmowe - Wymagania ogólne – Zasilacze – Parametry funkcjonalne i metody badań
- PN-93/E-08390/14 :1993 Systemy alarmowe - Wymagania ogólne – Zasady stosowania
- PN-EN 50131-1:2009 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe.
- PN-EN 50130-4 :2002 Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna
- Warunki Techniczne Wykonania i Odbioru Robót Budowlano - Montażowych cześć V Instalacje Elektryczne – wyd. Min. Bud. i Przem. Mat. Bud.
- PN-EN 60204-1 Bezpieczeństwo maszyn. Część 1: "Wymagania ogólne"
- Rozporządzenie Ministra Gospodarki z dnia 30 października 2002 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy w zakresie użytkowania maszyn przez pracowników podczas pracy (Dz.U. 2002 nr 191 poz. 1596).
- Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 4 września 2012 r. w sprawie podstawowych przepisów porządkowych związanych z zapewnieniem bezpieczeństwa i ochrony lotów oraz porządku na lotnisku (Dz. U. z 2012 r. poz. 1023)
- Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002
- Rozporządzenie Komisji (UE) nr 185/2010 z dnia 4 marca 2010 r., ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego ([Dz.U. L 55 z 5.3.2010)
- Rozporządzenie Komisji (UE) nr 72/2010 z dnia 26 stycznia 2010 r., ustanawiające procedury przeprowadzania inspekcji Komisji w zakresie ochrony lotnictwa (Dz.U. L 23 z 27.1.20100
- Rozporządzenie Komisji (UE) nr 1254/2009 z dnia 18 grudnia 2009 r. ustanawiające kryteria pozwalające państwom członkowskim na odstępstwo od wspólnych podstawowych norm ochrony lotnictwa cywilnego i przyjęcie alternatywnych środków w zakresie ochrony ([Dz.U. L 338 z 19.12.2009)
- Rozporządzenie Komisji (WE) nr 272/2009 z dnia 2 kwietnia 2009 r. uzupełniające wspólne podstawowe normy ochrony lotnictwa cywilnego określone w załączniku do

rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 (Dz.U. L 91 z 3.4.2009)

- Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (DzU 2005, nr 145, poz. 1221, Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 lipca 2005 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie osób i mienia)
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU 2007, nr 89, poz. 590 z poźn. zm.)
- Rozporządzenia Rady Ministrów z dnia 19 czerwca 2007 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego realizującego zasady ochrony lotnictwa (DzU 2007, nr 116, poz. 803)
- Obwieszczeniu nr 5 Prezesa Urzędu Lotnictwa Cywilnego dnia 9 sierpnia 2007 r. w sprawie listy przedmiotów zabronionych do wnoszenia na teren strefy zastrzeżonej lotniska i przewozu w bagażu kabinowym oraz rejestrowanym pasażera (Dz.Urz. ULC, nr 5 z 01.10.2007 r.)
- Rozporządzenie Ministra Infrastruktury z dnia 30 kwietnia 2004 r. w sprawie klasyfikacji lotnisk i rejestru lotnisk cywilnych, (DzU 2004, nr 122, poz. 1273)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 września 2005 r. w sprawie form kontroli bezpieczeństwa przeprowadzanej w zasięgu terytorialnym przejścia granicznego oraz w środkach komunikacji międzynarodowej przez funkcjonariuszy Straży Granicznej, (DzU 2005, nr 197, poz. 1642.)
- Ustawa z dnia 12 października 1990 r. o ochronnie granicy państwowej, (DzU 2005, nr 226, poz. 1944 ze zm.)
- Ustawa z dnia 12 października 1990 r. o Straży Granicznej, (DzU 2005, nr 234, poz. 1997 ze zm.)
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, (DzU2007, nr 89, poz. 590 z późn. zm.)
- Ustawa Prawo lotnicze, (DzU 2006, nr 100, poz. 696 z późn. zm.)

System Sygnalizacji Pożaru

Zaprojektowano system alarmu pożaru chroniący całą powierzchnie obiektu w klasie ochrony L1. System oparty na mikroprocesorowej centralce pożarowej pracującej w układzie linii dozorowych, pętlowych z możliwością indywidualnego adresowania wszystkich elementów. Instalacja sygnalizacji pożaru ma za zadanie między innymi sterowanie instalacją wentylacji pożarowej, zamykaniem przegród na granicach stref pożarowych, zamykaniem klap odcinających, sterowanie dźwigami osobowymi, sterowanie dźwiękowym systemem ostrzegawczym.

W skład systemu będą wchodziły następujące elementy :

centrala pożarowa,

optyczne i temperaturowe czujki dymu,

ręczne ostrzegacze pożaru ROP,

moduły sterujące,

moduły monitorujące,

izolatory zwarć.

Linie dozorowe w konfiguracji pętli wraz z izolatorami zwarć zapewniają wysoką odporność systemu na uszkodzenia linii dozorowej. Izolatory zostaną umieszczone w podstawach czujek i zostaną rozmieszczone zgodnie z zaleceniami producenta i obowiązującymi przepisami. Centrala systemu alarmu pożaru wyposażona będzie w panel z wyświetlaczem, drukarkę zdarzeń, będzie umożliwiała wysłanie sygnału o pożarze i awarii do PSP za pomocą dodatkowego urządzenia UTA. Do wykrywania pożaru przewidziano zastosowanie optycznych i termicznych czujek dymu. Zastosowane czujki przetwarzają informacje o stanie przestrzeni pomiarowej w formie analogowej, dzięki czemu ich czułość dostosowuje się do zmian środowiskowych (temperatura, wilgotność, ciśnienie), jak również do postępującego zabrudzenia układów pomiarowych. Powyższe właściwości pozwalają na zmniejszenie prawdopodobieństwa powstania alarmów symulacyjnych (fałszywych), jak również częstotliwości dokonywania czynności konserwacyjnych. Do wywoływania alarmu pożarowego przez osoby przebywające w obiekcie przewidziano ręczne ostrzegacze pożaru rozmieszczone przy wyjściach ewakuacyjnych z kondygnacji objętej ochroną. Odległość między ręcznymi ostrzegaczami pożarowymi nie przekracza 30 m. Funkcje sterownicze oraz monitorujące instalacji SAP realizowane będą przez moduły sterujące i monitorujące. Moduły te umożliwiają przekazanie do centrali sygnałów dyskretnych, w celu ich dalszej interpretacji lub sterowanie stykiem bezpotencjałowym. Dzięki zastosowaniu oporników końcowych, wejścia są monitorowane, a ewentualne uszkodzenie połączeń (przerwa lub zwarcie) - sygnalizowane przez centralę. Dla wszystkich elementów sterujących i monitorujących przewiduje się zastosowanie izolatorów zwarć.

Zakres opracowania

Niniejszy dokument obejmuje projekt Systemu Sygnalizacji Pożarowej (SSP):

- detekcję pożaru czujkami automatycznymi i ręcznymi ostrzegaczami pożarowymi
- rozgłaszanie sygnałów ewakuacyjnych poprzez uruchomienie właściwych linii sygnalizatorów Dźwiękowego Systemu Ostrzegawczego (DSO)
- zamykanie klap pożarowych w budynku,
- wysterowanie systemów automatyki wentylacji i klimatyzacji,
- uruchamianie systemów wentylacji pożarowej,
- odblokowanie rygli systemu kontroli dostępu

Projekt obejmuje wykonanie tras kablowych pętli dozorowych linii sterujących oraz monitorujących. Dla potrzeb systemu sygnalizacji pożarowej w części objętej wyżej wymienionym zakresem przewidziano zastosowanie następujących urządzeń:

- centrala sygnalizacji pożarowej,
- automatyczne i ręczne ostrzegacze pożarowe techniki pętlowej,
- moduły wejścia/wyjścia do sterowania i nadzorowania urządzeń ppoż.

Zastosowane w projekcie urządzenia posiadają aktualne certyfikaty, deklaracje zgodności i świadectwa dopuszczenia zgodnie z obowiązującym prawem na terenie Rzeczpospolitej Polskiej.

Opis systemu

Projekt systemu sygnalizacji pożarowej wykonano zgodnie z założeniami przyjętymi w projekcie budowlanym instalacji sygnalizacji pożarowej w zakresie ochrony całkowitej budynku. Ze względu na konieczność przyjęcia do obliczeń konkretego rozwiązania analizę i obliczenia oparto na systemie Integral IP firmy Schrack Seconet. Do realizacaji można przyjść inny, równoważny system. Będzie to wymagało wykonania oblcizeń na parametrach technicznych przyjętego systemu.

Centrala sygnalizacji pożarowej

W celu zapewnienia najwyższego poziomu bezpieczeństwa pracy systemu sygnalizacji pożarowej zastosowano centrale sygnalizacji pożarowej posiadającą redundancję sprzętową i programową wszystkich kart (tzn. zdublowanie wszystkich układów z możliwością przełączania w czasie awarii), a także układów pamięci gdzie przechowywane jest oprogramowanie odpowiedzialne za prawidłową pracę central. Zastosowanie takiego rozwiązania gwarantuje, że cały system bezpieczeństwa będzie funkcjonował w sposób niezawodny nawet w przypadku

awarii jego poszczególnych podzespołów. W takim przypadku system będzie nie tylko zdolny do wykonywania podstawowych funkcji awaryjnych zgodnie z PN-EN 54-2 ale będzie realizował wszystkie funkcje kontrolno-sterujące zgodnie ze scenariuszem rozwoju zdarzeń w trakcie pożaru. W przypadku wystąpienia awarii systemowej nastąpi przełączenie systemu podstawowego na układ zapasowy, realizujący wszystkie funkcje systemu podstawowego (100 % redundancja). W każdej obudowie centrali sygnalizacji pożarowej znajdują się zatem dwa równoważne systemy mikroprocesorowe, z czego jeden pełni rolę wiodącą, a drugi jest systemem zapasowym pracującym w trybie gorącej rezerwy. Integral IP jest systemem o 32 – bitowej architekturze. Dzięki wykorzystaniu układów o bardzo dużym stopniu integracji (technologia Microvia), centrala ta posiada ogromną moc obliczeniową mimo niewielkich rozmiarów. Integral IP to system sygnalizacji pożarowej charakteryzujący się strukturą zdecentralizowaną, oparty jest o budowę modułową, projektowaną i programowaną stosownie do wymogów stawianych konkretnej instalacji sygnalizacji pożarowej.

Centrale sygnalizacji pożarowej posiadają pamięć zdarzeń o pojemności 65 tyś zdarzeń oraz dodatkową pamięć blokowaną przed zapisem (tzw. „czarna skrzynka") z programowalnym czasem blokady i ilości zapisywanych zdarzeń. Rozbudowane układy pamięci pozwalają na bieżąca analizę pracy systemu i do ewentualnego ustalenia powstania pożaru i sposobu działania urządzeń ppoż. Zapisane zdarzenia mogą być przeglądane na panelu obsługi centrali oraz drukowane na taśmie papierowej, w sposób uporządkowany według daty i czasu wystąpienia zdarzenia, za pomocą wbudowanej drukarki lub przy użyciu narzędzi serwisowych odczytane i wydrukowane na papierze A4.

Każda centrala w konfiguracji podstawowej składa się z następujących podzespołów:

- obudowy z blachy stalowej z wycięciem na panel obsługi lub bez
- karty głównego procesora
- zasilacza
- kasety z magistralami systemowymi
- panelu obsługi
- zacisków sieciowych oraz kabli akumulatora
- miejsca montażu dla akumulatora

Wyniesione panele wskazań i obsługi

Do centrali można za pośrednictwem magistrali podłączyć urządzenia zewnętrzne takie jak wyniesione panele obsługi. Magistrala z szeregową transmisją danych.

Zadaniem projektowanego systemu jest możliwie szybkie powiadomienie odpowiedzialnych służb znajdujących się w pomieszczeniu Ochrony.

Informacja zawierać będzie dokładną lokalizację pożaru w postaci adresu alarmującego elementu oraz dodatkowego opisu pomieszczenia/obszaru na wyświetlaczu ciekłokrystalicznym centrali sygnalizacji pożarowej i na wydruku drukarki protokołującej.

Integracja z BMS/SMS, zarządzanie i wizualizacja, zdalny dostęp

Zastosowanie technologii IP umożliwia elastyczne przyłączanie do systemu zewnętrznych systemów: systemu automatyki budynku (BMS), systemu zarządzania bezpieczeństwem (SMS). Istnieje możliwość wykorzystania protokołu komunikacyjnego systemu SAP lub podłączenia systemu zewnętrznego w standardzie OPC, BACnet lub MODBUS z wykorzystaniem dedykowanego gateway-a.
Centrala może wysyłać emaile z komunikatami alarmowymi do użytkowników systemu lub serwisu.

Elementy peryferyjne

System SSP opiera się na technice linii pętlowych umożliwiających podłączenie do 250 elementów peryferyjnych na jednej pętli dozorowej o długości maksymalnej równej 3500 m. Wszystkie elementy pracujące w pętli dozorowej posiadają obustronne izolatory zwarć, które całkowicie eliminują ryzyko utraty nadzoru nad strefą chronioną (każdy uszkodzenie na pętli dozorowej takie jak zwarcie lub przerwa jest odizolowane prze izolatory zwarć).
Jednym z najważniejszych elementów peryferyjnych jest interaktywna czujka multisensorowa która może pracować jako czujka dymu, ciepła lub jako czujka multisensorowa. Wielokryteryjne czujki zdolne są wykrywać pożary w klasach – od TF1 do TF9. Regulowana czułość części optycznej, aż 9 klas czułości członu temperaturowego oraz zastosowanie interaktywnej technologii która dostosowuje czułość czujki do parametrów otoczenia sprawiają, że urządzenia te spełnią nawet najtrudniejsze wymagania stawiane tego typu elementom przez użytkowników.

Dobór urządzeń systemu sygnalizacji pożarowej

Centrale sygnalizacji pożarowej, panele wskazań i obsługi

Ze względu na konieczność przyjęcia do obliczeń konkretego rozwiązania analizę i obliczenia oparto na systemie Integral IP firmy Schrack Seconet. Do realizacaji można przyjść inny, równoważny system. Będzie to wymagało wykonania oblcizeń na parametrach technicznych przyjętego systemu. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza

konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności system.

Wszystkie zdarzenia są zapisywane w pamięci centrali/central. Na drukarce systemowej lub z poziomu systemu wizualizacji i zarządzania istnieje możliwość wydruku wybranych zdarzeń systemowych.

Do obsługi systemu przewidziano wyniesiony panel obsługi zlokalizowany w pomieszczeniu 1.60 Dyżurnego Portu. Zewnętrzny panel obsługi (składający się z sześciowierszowego wyświetlacza LCD) umożliwia wyświetlanie do 40 znaków w jednej linii i służy do informowania o wszystkich stanach systemu za pomocą alfanumerycznych tekstów informacyjnych. Panel wyposażony jest w wewnętrzna drukarkę drukująca każde zdarzenie z indywidualnym tekstem użytkownika i dokładnym czasem wystąpienia zdarzenia.

W zaprojektowanym zewnętrznym panelu obsługi łącze danych oraz przewody zasilania są zdublowane – spełnienie wymagań normy PN-EN 54-2 p. 12.5.

Elementy peryferyjne

Elementy peryferyjne systemu sygnalizacji pożarowej pracują w układzie linii dozorowych pętlowych z indywidualnym adresowaniem następujących elementów:

- interaktywnych punktowych czujek multisensorowych (TF1 do TF9) w projekcie oznacznych symbolem CUBUS MTD 533X (dla ustakenie r ownowazności będzie brany pod wuwagę: zakres dedekcji TF1 do TF9, sensor dymu i temperatry)
- systemów wczesnej detekcji dymu (systemów zasysających z czujnikiem dymu o podwyższonej czułości): do analizy przyjęto AirSCREEN ASD 535, można zastosować rozwiązanie równoważne pod warunkiem wykonania obliczeń na podstawie parametrów przyjętego do realizacjii systemu systemu,
- ręcznych ostrzegaczy pożarowych wewnetrznych w projekcie oznacznych symbolem MCP 545X i zewnętrznych w projekcie oznacznych symbolem MCP 535X,
- modułów sterujących we/wy:
    - 2 wyjścia przekaźnikowe z funkcją sprzężenia zwrotnego, 4 wejścia nadzorowane, możliwa jednoczesna kontrola do 32 modułów na pętlę , Programowalna pozycja w razie uszko-dzenia (fail – safe) , zintegrowany izolator zwarć, obudowa IP 66 w projekcie oznacznych symbolem BX-O2I4
    - wyjście przekaźnikowe z programowalną pozycją w razie uszkodzenia (fail – safe), 2 wejścia dla nadzorowania zestyków bezpotencjałowych, wejście z

optozłączem, zintegrowany izolator zwarć, obudowa IP 66 w projekcie oznacznych symbolem BX-OI3

Wszystkie zaprojektowane w systemie elementy pracujące w pętlach dozorowych wyposażone są w obustronne izolatory zwarć dla uzyskania wysokiej odporności systemu na uszkodzenia typu „przerwa" lub „zwarcie" w pętli dozorowej.

Pełna adresowalność instalacji sygnalizacji pożarowej umożliwia m. in. identyfikację miejsca pożaru z dokładnością do pojedynczego punktu adresowego, tj. czujki lub ręcznego ostrzegacza pożarowego, a także programowe przypisanie funkcji wykonawczych (sterujących) i funkcji monitorujących poszczególnym adresowanym wyjściom sterującym i wejściom monitorującym w modułach włączonych w pętle dozorowe i zainstalowanych w różnych miejscach obiektu.

Nie przewiduje się zastosowania w obiekcie czujek z izotopem promieniotwórczym.

Programowanie wszystkich elementów peryferyjnych, jak również kontrola poprawności połączeń fizycznych między nimi przeprowadzane są z jednego miejsca, za pomocą komputera klasy PC (notebook). Wszystkie czujki i przyciski będą posiadały indywidualny adres w systemie, co pozwoli na dokładną lokalizację punktu, z którego może zostać wywołany alarm. Każdy element w instalacji, w tym grupy dozorowe, detektory, przyciski, elementy sterujące, zostaną opisane w centrali indywidualnymi tekstami, dostosowanymi do potrzeb użytkownika. Adresowalny system sygnalizacji pożarowej umożliwia detekcję pożaru z dokładnością do pojedynczej czujki. Dodatkowo zastosowanie w każdym elemencie pętlowym obustronnego zintegrowanego izolatora zwarć umożliwia swobodne prowadzenie linii pętlowej przez różne strefy pożarowe, dowolne definiowanie grup dozorowych w systemie z możliwością logicznego polaczenia w grupę dozorową elementów zainstalowanych na różnych pętlach.

Zakres ochrony systemu sygnalizacji pożarowej

Zakres ochrony, jak i rozmieszczenie czujek wykonano zgodnie z założeniami przyjętymi w projekcie budowlanym.

W obiekcie zabezpieczeniem SSP podlegają przestrzenie właściwe (z wyjątkiem pomieszczeń sanitarnych), klatki schodowe, korytarze, pomieszczenia techniczne i przestrzenie międzystropowe.

Instalacja sygnalizacji pożarowej obejmuje ochroną wszystkie pomieszczenia właściwe wraz z ich przestrzenią międzystropową czujkami uniwersalnymi o szerokim spektrum wykrywania pożarów (od TF1 do TF9).

Ręczne uruchomienie sygnału alarmu ogólnego II stopnia będzie następowało poprzez ręczne ostrzegacze pożarowe. Ponadto zastosowano elementy sterowania i kontroli

montowanych bezpośrednio w liniach dozorowych (moduły wyposażone w wejścia nadzorowane i wyjścia sterujące) celem realizacji funkcji sterowniczych i kontrolnych. Realizacja funkcji wykonawczych następuje automatycznie po wykryciu przez centralę zagrożenia pożarowego. W przypadku wykrycia zagrożenia pożarowego SSP będzie przesyłał sygnały:

- uruchamiające odpowiednie linie alarmowe DSO,
- zamykające klapy pożarowe w kanałach wentylacyjnych,
- wyłączające centrale wentylacyjne i klimatyzacyjne,
- załączające wentylatory napowietrzające,
- zwalniające kontrole dostępu w drzwiach na drodze ewakuacji.

Sterowanie wyłączaniem central wentylacyjnych, otwieraniem klap oddymiających, otwieranie drzwi stanowiących wyjścia ewakuacyjne czy załączanie emisji komunikatów alarmowych obsługiwane jest poprzez odpowiednie wyjścia przekaźnikowe centrali systemu Integral IP lub pętlowe moduły sterujące.

Instalacja pętli dozorowych

Elementy peryferyjne takie jak: czujki pożarowe, ręczne ostrzegacze pożarowe oraz moduły wejścia/wyjścia są elementami pętlowymi nieprzerwanie komunikującymi się z centralą sygnalizacji pożarowej. Każdy element pętli dozorowej jest wyposażony w zintegrowany obustronny izolator zwarć i w przypadku awarii pętli (zwarcie, przerwa) może być zasilany z dwóch stron.

Pętle dozorowe, na których zamontowane zostaną czujki pożarowe, ręczne ostrzegacze pożarowe oraz moduły wejścia/wyjścia zostaną rozprowadzone w całym obiekcie.

Dla potrzeb zgrubnej identyfikacji miejsca pożaru oraz dla potrzeb ich powiazania z wyjściami sterującymi elementy detekcyjne zostały podzielone na grupy dozorowe zgodnie z planowanym podziałem funkcjonalnym obiektu:

W celu szczegółowej identyfikacji miejsca zagrożenia pożarem na etapie programowania centrali, należy przypisać do każdej czujki indywidualne teksty opisujące lokalizację czujki zgodnie z opisem pomieszczeń zawartym projekcie budowlanym (np. numer i nazwa pomieszczenia lub przeznaczenie).

Zaprojektowano 6 pętli dozorowych. Instalacje wykonano przyjmując następujący podział elementów na poszczególne pętle:

Pętla 1 została zaprojektowana do ochrony kanału kablowego. Na tej pętli zostały zaprojektowane czujki o podwyższonym stopniu IP wraz z gniazdami hermetycznymi.

Na pętli nr 3 znajduje się moduł pętlowy obsługujący system zasysający chroniący przestrzeń podłogową w części zachodniej piętra 1.

Pętla dozorowa	Czujka multisensorowa	Ręczny ostrzegacz pożarowy jednostadiowy	Moduł monitorująco-sterujący BX-O2I4	Moduł monitorująco-sterujący BX-OI3	Ręczny ostrzegacz pożarowy dwunostadiowy	Moduł pętlowy do systemu zasysającego
P1	25	0	0	0	0	0
P2	111	17	4	7	0	0
P3	88	11	0	6	0	0
P4	96	6	5	7	5	1
P5	73	4	0	6	0	0
P6	101	0	0	18	0	0
Razem	**494**	**38**	**9**	**44**	**5**	**1**

Dobrane ilości elementów (czujek, ROP-ów, wejść, wyjść, itp.) nie przekraczają maksymalnych dopuszczalnych ilości wynikających z dokumentacji techniczno-ruchowej producenta.

Obliczenia

Bilans prądowy central

Integral - Bilans prądowy

SCHRACK SECONET

Projekt: Mazury — dotyczy IRP 7.2

Projekant: Qwer — Data obliczeń: 2013-11-02

Konfiguracja akumulatorów:

Typ akumul.:	CTM CT44-12	Poj. znamionowa:	44 Ah	Prąd zasilacza:	7 A
Liczba par:	1	Poj. efektywna:	44 Ah	Czas buforowania:	72 h
		Poj. całkowita:	44 Ah	Czas buforowania - systemy specjalne:	72 h

Komponenty CSP

			Prąd dozoru:	Prąd alarmu:
Panel obsługi:	(pusty)		0,00	19,00
Slot 1	B5-MCU		35,00	35,00
Slot 2	B5-NET2-485		120,00	120,00
Slot 3	B5-DXI2		35,00	35,00
Slot 4	B5-DXI2		35,00	35,00
Slot 5	B5-DXI2		35,00	35,00
Slot 6	(pusty)		0,00	0,00
Slot 7	(pusty)		0,00	0,00
Slot 8	(pusty)		0,00	0,00
Slot 9	B5-BAF	☑ MMI Bus w użyciu	32,50	32,50
Slot 10	B5-PSU		31,00	31,00

Slot 11,12,13 B3-RELx - Obciążenie pomijalne - prądowy impuls przełączajacy 9 mA w czasie 10 ms

Urządzenia na MMI-BUS:

	Prąd dozorowy:	Prąd alarmu:	Ilość:	Prąd dozoru:	Prąd alarmu:
B5-MMI-CIP (pole MAP)	46,500	46,500		0,00	0,00
B5-MMI-CPP (pole MAP z drukarką)	50,000	50,000	1	50,00	50,00
B5-MMI-HCIP (pole High-End)	97,000	97,000		0,00	0,00
B3-MMI-EAT64, B3-MMI-IPEL	28,000	28,000		0,00	0,00
B3-MMI-EAT32, B3-MMI-IPES	14,000	14,000		0,00	0,00
B3-MMI-FPA (Austria)	14,000	30,000		0,00	0,00
B3-MMI-FPS (Szwecja)	14,000	14,000		0,00	0,00
B3-MMI-UIO	14,000	14,000		0,00	0,00
B3-MMI-FAT (Niemcy)	14,000	14,000		0,00	0,00
B3-MMI-IPS (Szwecja)	14,000	14,000		0,00	0,00
B3-MMI-CIP (pole Integral)	20,000	38,000		0,00	0,00
B3-MMI-CIP-VdS (pole Integral)	38,000	38,000		0,00	0,00
B3-MMI-CPP (pole Integral z drukarką)	21,500	21,500		0,00	0,00
B3-MMI-CPP-VdS (pole Integral z drukarką)	39,500	39,500		0,00	0,00

Pomijalny pobór prądu przez diody na tablicach EAT - brak obciążenia w trybie normalnej p

Prąd sumaryczny CSP: **373,50** **392,50 mA**

Integral - Bilans prądowy

SCHRACK SECONET

Projekt: Mazury

dotyczy IRP 7.2

Projekant: Qwer

Data obliczeń: 2013-11-02

Peryferia:

B3-MTI8 (technika monologowa)	Prąd dozorowy:	Prąd alarmu:		Ilość:	Prąd dozoru:	Prąd alarmu:
(maks. 3 alarmy na linię)			max./linię			
SLK-EN	0,035	40,00	0		0,00	0,00
DCC-1E	0,035	50,00	0		0,00	0,00
DFE-60E	0,000	50,00	0		0,00	0,00
DFE-90E	0,000	50,00	0		0,00	0,00
HF-24E	0,200	50,00	0		0,00	0,00
DKM MBM (przycisk przelotowy)	0,000	35,00	0		0,00	0,00
DKM MTM (przycisk końcowy)	0,800	43,00	0		0,00	0,00
BSI (gniazdo przelotowe)	0,010	35,00	0		0,00	0,00
TMI (gniazdo końcowe)	0,800	37,00	0		0,00	0,00
BSS (moduł przelotowy)	0,000	35,00	0		0,00	0,00
TMS (moduł końcowy)	0,800	37,00	0		0,00	0,00
			Prąd sumaryczny:		**0,00**	**0,00 mA**

B3-DAI2	Prąd dozorowy:	Prąd alarmu:		Ilość:	Prąd dozoru:	Prąd alarmu:
(maks. 3 alarmy na pętlę przy wsp. 0,7)			max./pętlę			
OSD 2000 (SSD 531K - LKM 531)	0,190	5,00	0		0,00	0,00
DMD 2000	0,150	5,00	0		0,00	0,00
Schrack STD 531	0,190	5,00	0		0,00	0,00
CUBUS MTD 533	0,235	5,00	0		0,00	0,00
CUBUS MTD 533X	0,120	2,50	0		0,00	0,00
BA-UPI	0,000	1,00	0		0,00	0,00
BX-UPI	0,000	1,00	0		0,00	0,00
BA-API	0,000	5,00	0		0,00	0,00
MCP 535X	0,090	2,50	0		0,00	0,00
MCP 545X	0,090	2,50	0		0,00	0,00
BA-AIM	0,500	0,50	0		0,00	0,00
BX-AIM	0,460	0,46	0		0,00	0,00
BA-OI3	0,460	0,46	0		0,00	0,00
BA-IOM	0,450	0,45	0		0,00	0,00
BA-IM4	0,460	0,46	0		0,00	0,00
BA-REL4	0,460	0,46	0		0,00	0,00
BA-RGW	0,950	0,95	0		0,00	0,00
SDI 82A	0,500	10,00	0		0,00	0,00
BA-SOL (low)	0,495	2,40	0		0,00	0,00
BA-SOL (high)	0,495	4,80	0		0,00	0,00
BA-FOL	0,474	6,50	0		0,00	0,00
BX-OI3	0,550	0,550	0		0,00	0,00
BX-O2I4	0,630	0,630	0		0,00	0,00
BX-IOM	0,430	0,430	0		0,00	0,00
BX-IM4	0,450	0,45	0		0,00	0,00
BX-REL4	0,510	0,51	0		0,00	0,00
BX-RGW	0,950	0,950	0		0,00	0,00
BX-ESL	0,400	0,400	0		0,00	0,00
BX-SOL (low)	0,495	2,40	0		0,00	0,00
BX-SOL (high)	0,495	4,80	0		0,00	0,00
BX-FOL	0,474	3,70	0		0,00	0,00

Integral - Bilans prądowy

SCHRACK SECONET

Projekt: Mazury

dotyczy IRP 7.2

Projekant: Qwer

Data obliczeń: 2013-11-02

B3-DCI6	Prąd dozorowy:	Prąd alarmu:	Ilość:	Prąd dozoru:	Prąd alarmu:
(maks. 1 alarm na linię)					
Ilość podłączonych linii:	2,000	2,000		0,00	0,00
Liczba detektorów:	0,000	21,000		0,00	0,00
LPL PIN	0,000	6,000		0,00	0,00
			Prąd sumaryczny:	**0,00**	**0,00 mA**

Integral - Bilans prądowy

SCHRACK SECONET

Projekt: Mazury

dotyczy IRP 7.2

Projekant: Qwer

Data obliczeń: 2013-11-02

B3-DTI2	Prąd dozorowy:	Prąd alarmu:	Ilość:	Prąd dozoru:	Prąd alarmu:
(maks. 3 alarmy na pętlę)			maks./pętlę		
B2-DBA	0,100	0,800		0,00	0,00
HF-24E	0,200	250,000	0	0,00	0,00
DCA-E	0,000	0,800	0	0,00	0,00
SIH-E	0,025	250,000	0	0,00	0,00
SLK-EN	0,035	40,000	0	0,00	0,00
DCC-1E	0,035	50,000	0	0,00	0,00
DFE-60E/90E	0,000	0,800	0	0,00	0,00
B3-DOI2	1,600	1,600	0	0,00	0,00
B2-DI2	2,500	2,500	0	0,00	0,00
B2-DOM	1,600	1,600	0	0,00	0,00
B2-DIM	3,000	3,000	0	0,00	0,00
B2-DBM			0	0,00	0,00
			Prąd sumaryczny:	**0,00**	**0,00 mA**

Integral - Bilans prądowy

SCHRACK SECONET

Projekt: Mazury — dotyczy IRP 7.2

Projekant: Qwer — Data obliczeń: 2013-11-02

Inne urzadzenia

Pozostałe urządzenia zasilane z zasilacza centrali:

		Prąd dozoru:	Prąd alarmu:	
(np. sygnalizatory, czujki liniowe dymu, trzymacze drzwiowe,...)	Prąd sumaryczny:			mA

Urządzenia specjalne

Urządzenia zasilane z zasilacza centrali zgodnie z normą TRVB 123:

		Prąd dozoru:	Prąd alarmu:	
(np. Systemy zasysające, ...)	Wprowadź dane:			mA

		Prąd dozoru:	Prąd alarmu:	
WYNIKI	**SUMA:**	**0,506**	**0,603**	**A**
minimalny prąd ładowania (80% w 24h)	pojemność znamionowa * 0,05		**2,200**	**A**
wymagana pojemność akumul. "dozorowanie"	prąd dozorowy * czas buforowania w st. dozorowania		**36,460**	**Ah**
wymagana pojemność akumul. "dozorowanie SDS"	prąd dozorowy * prąd dozorowy SDS * czas buforowania w st. doz(		**0,000**	**Ah**
wymagana pojemność akumul. "alarmowanie"	prąd alarmowy * czas buforowania w st. alarmu		**0,302**	**Ah**
wymagana pojemność akumul. Suma (d+a)	("Dozorowanie" + "Dozorowanie CZS" +"Alarmowanie")		**36,761**	**Ah**
dostępny prąd alarmowy	maks. prąd zasilacza - prąd w st. alarmowania		**6,397**	**A**
dostępny, buforowany prąd w stanie dozor.	(efektywna poj. akumul. - wym. poj. akumul.)/czas buforowania		**0,101**	**A**
dostępny, niebuforowany prąd w st. dozor.	maks. prąd zasilacza - prąd dozor. - min. prąd ładowania		**4,294**	**A**
maks. wartość na zaciskach pomiar. PSU5	(50mV/A)		**96,00**	**mV**
wartość pomiarowa na zasilaczu PSU5	(50mV/A)		**25,32**	**mV**
czas buforow. (dozorowanie + alarm)			**OK**	
ładowanie do 80% poj. akum. w 24h			**OK**	

Do obliczeń w bilansie prądowym przyjęto czas pracy na akumulatorach w stanie spoczynku równy 72h zaś czas pracy na akumulatorach w stanie alarmu równy 0,5h. Czas naładowania rozładowanych baterii do wartości 80% wynosi 24 godziny.

Kalkulacja poszczególnych pętli dozorowych wraz z dopuszczalnymi długościami

Project: **SCHRACK BMZ INTEGRAL X-line calculation** **Planner:**

Typ	Nr	Pętla Tryb	OP	LED	Kabel A mm²	I_{LED} mA	Dym/Temp MTD533X	ROP MCP545X	We/Wy BX-O2I4	We/Wy BX-OI3	ROP MCP535X	ASD 535-x XLM35	Linia DC BX-AIM	We/Wy BX-IOM	We/Wy BX-O1	We/Wy BX-I2	Syrena BX-SOL	suma ilość urządzeń	gwarantowana długość [m]	typowa długość [m]	R_{CCmess} [Ω]	≈Długość [m]	wynik	Uwagi, np. zakres grup, itp.
DXI	1	Pętla AUTO	3	0,5	12,0	25											25	3500	3500		0	OK (XLINE)	
																			1500	1500				
	2	Pętla AUTO	3	0,5	12,0	111	17	4	7								139	2683	3500		0	OK (XLINE)	
																			1500	1500				
DXI	3	Pętla AUTO	3	0,5	12,0	88	11		6								105	3500	3500		0	OK (XLINE)	
																			1500	1500				
	4	Pętla AUTO	3	0,5	12,0	96	6	5	7	5	1						120	2945	3500		0	OK (XLINE)	
																			1500	1500				
DXI	5	Pętla AUTO	3	0,5	12,0	73	4		6								83	3500	3500		0	OK (XLINE)	
																			1500	1500				
	6	Pętla AUTO	3	0,5	12,0	101			18								119	2806	3500		0	OK (XLINE)	
																			1500	1500				
DXI	7	Pętla AUTO	3	0,5	12,0												0	3500	3500		0	OK (XLINE)	
																			1500	1500				
	8	Pętla AUTO	3	0,5	12,0												0	3500	3500		0	OK (XLINE)	
																			1500	1500				
DXI	9	Pętla AUTO	3	0,5	12,0												0	3500	3500		0	OK (XLINE)	
																			1500	1500				
	10	Pętla AUTO	3	0,5	12,0												0	3500	3500		0	OK (XLINE)	
																			1500	1500				
DXI	11	Pętla AUTO	3	0,5	12,0												0	3500	3500		0	OK (XLINE)	
																			1500	1500				
	12	Pętla AUTO	3	0,5	12,0												0	3500	3500		0	OK (XLINE)	
																			1500	1500				
DXI	13	Pętla AUTO	3	0,5	12,0												0	3500	3500		0	OK (XLINE)	
																			1500	1500				
	14	Pętla AUTO	3	0,5	12,0												0	3500	3500		0	OK (XLINE)	
																			1500	1500				
Suma:							494	38	9	44	5	1	0	0	0	0	0	591						

Dla przedstawionego wcześniej podziału elementów na poszczególne pętle dozorowe oraz przy dobraniu przewodu YnTKSYekw 1x2x0,8mm maksymalne dopuszczalne długości pętli dozorowych nie przekraczają projektowanych długości pętli.

Algorytmy sterowań

Przewiduje się, że system sygnalizacji pożarowej pracować będzie w trybie alarmowania dwustopniowego.

Definicje

Dwustopniowa organizacja alarmowania

W celu eliminacji fałszywych alarmów z czujek automatycznych oraz umożliwienia służbom dozoru zneutralizowania niewielkiego zagrożenia pożarowego bez konieczności wzywania Jednostki Ratowniczo-Gaśniczej Straży Pożarnej, przyjęto dwustopniową procedurę organizacji alarmowania. Przy tak przyjętej procedurze zagrożenie wykryte przez czujkę automatyczną powoduje jedynie sygnalizację alarmu pożarowego I stopnia.

Alarm pożarowy I stopnia

Jest to alarm sygnalizowany jedynie na panelu 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 jednostki Państwowej Straży Pożarnej. Dodatkowo wysterowane zostają urządzenia automatyki pożarowej zgodnie z matrycą sterowań wynikającą ze scenariusza rozwoju zdarzeń na wypadek pożaru.

Czas potwierdzenia

Po zgłoszeniu przez SSP alarmu I stopnia, służby dozoru mają obowiązek potwierdzenia przyjęcia informacji o zagrożeniu pożarowym oraz o podjętej interwencji. Przyjęto, że czas potwierdzenia wynosi 30 sekund. W tym czasie pracownik ochrony musi podejść do centrali i wcisnąć przycisk *ROZPOZNANIE* na panelu obsługi. Po upływie tego czasu

bez potwierdzenia 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 nią 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 drugi z pracowników służb dozoru po dotarciu na miejsce zagrożenia podejmuje decyzję o konieczności wezwania Jednostek Ratowniczych PSP lub próbie neutralizacji zagrożenia we własnym zakresie. W pierwszym przypadku niezbędne jest wciśnięcie najbliższego ROPa lub przekazanie informacji do pracownika pełniącego dozór w celu wciśnięcia ROPa zlokalizowanego w pomieszczeniu ochrony. W przypadku możliwości podjęcia akcji gaśniczej we własnym zakresie niezbędne jest przekazanie informacji do pracownika pełniącego dozór w pomieszczeniu ochrony w celu skasowania alarmu przed upływem czasu rozpoznania. W przypadku braku jakiejkolwiek reakcji (potwierdzenie ROPem lub skasowanie alarmu) po czasie rozpoznania system przechodzi automatycznie w alarm II stopnia.

Opis współpracy systemu sygnalizacji pożarowej z innymi instalacjami w obiekcie – sterowanie i monitorowanie

W opisie sterowań przedstawiono zasady sterowań poszczególnymi urządzeniami automatyki pożarowej.

Przesyłanie informacji do PSP

Centrala sygnalizacji pożarowej została przystosowana do połączenia z lokalną jednostką Państwowej Straży Pożarnej za pośrednictwem Urządzenia Transmisji Alarmów (UTA). Z nadajnikiem UTA, CSP została połączona bezpośrednio. Centrala umożliwia przesyłanie sygnałów alarmu ogólnego II stopnia, oraz sygnału ogólnego uszkodzenia systemu poprzez zamknięcie odpowiednich styków przekaźnikowych w CSP.

Sposób transmisji sygnałów z UTA do stacji monitoringu oraz sam nadajnik UTA dostarczony zostanie przez firmę specjalizującą się w monitoringu i transmisji alarmów w przypadku podpisania stosownej umowy przez użytkownika obiektu z firmą świadczącą usługę transmisji sygnałów do Straży Pożarnej.

Połączenie między CSP a UTA należy wykonać kablem YnTKSYekw 1x2x0,8mm.

Przesyłanie informacji do LSP

Centrala ma możliwość podłączenia panelu wyniesionego dla potrzeb Lotniskowej Straży Pożarnej. Poza zakresem niniejszego opracowania.

Sterowanie DSO

System sygnalizacji pożarowej realizuje sterowanie Dźwiękowego Systemu Ostrzegawczego za pomocą karty przekaźnikowej zainstalowanej bezpośrednio w centrali. W przypadku wystąpienia zdarzenia pożarowego SSP uaktywnia odpowiednie styki bezpotencjałowe karty odpowiedzialne za uruchomienie odpowiednich linii DSO. Instalację sterowania instalacją DSO należy wykonać kablem YnTKSY 1x2x0,8mm

Sterowanie centralami wentylacji bytowej

Przyjęto, ze w wyniku alarmu II stopnia będzie następowało wyłączenie wentylacji bytowej. Do sterowania rozdzielniami przewidziano moduły sterujące w najbliższym sąsiedztwie szaf sterujących i zasilających centrale wentylacyjne i wentylatory.

Wyłączenie central wentylacyjnych będzie odbywało się poprzez otwarcie styku odpowiednich przekaźników układów sterujących zlokalizowanych we właściwej tablicy sterującej centralą wentylacyjną.

Instalację sterowania centralami wentylacji komfortu należy wykonać kablem YnTKSYekw 1x2x0,8mm.

Sterowanie zamykaniem klap odcinających wentylacji bytowej

W stanie normalnej pracy instalacji wentylacji i klimatyzacji klapy odcinające będą znajdować się w pozycji otwartej dzięki podanemu napięciu. Zamknięcie klap będzie odbywało się w wyniku alarmu ogólnego II stopnia. Klapy wentylacji bytowej zostaną zamknięte poprzez odcięcie zasilania modułami sterującymi SSP.

Instalację sterowania i monitorowania centralami wentylacji bytowej należy wykonać kablem YnTKSYekw 1x2x0,8mm.

Sterowanie oddymianiem grawitacyjnym i systemem zapobiegania zadymieniu na klatce schodowej

Obszar obiektu obejmuje trzy strefy dymowe: SD „A”, SD „B”, SD „C” oddymianych grawitacyjnie, obejmujących przyziemie oraz antresolę. W analizowanym obszarze obiektu występują ruchome (między osiami 10d -11,b w osi Ba) i stałe kurtyny dymowe. Kurtyna

dymowa sterowana jest modułem sterującym systemu sygnalizacji pożaru. Oddymianie realizowane jest za pomocą klap dymowych zlokalizowanych w świetlikach dachu, o powierzchni czynnej 20 m^2 dla każdej strefy dymowej. Każde pasmo świetlików składa się z 6 klap oddymiających dwuskrzydłowych. Każda klapa wyposażona jest w zespół dwóch siłowników (dobór w projekcie architektonicznym) o poborze prądu 4A na każdą klapę. Łączny pobór prądu dla jednego pasma świetlików wynosi 24 A.
Dla każdego pasma świetlików zaprojektowano centralę oddymiającą o wydajności prądowej 24A. W projekcie do obliczeń przyjęto centralę AFG-2004/24A 3L3G. Centrale są sterowane i monitorowane za pomocą modułów kontrolno-sterujących systemu sygnalizacji pożaru. Dla każdej centrali przewidziano jeden moduł.

Instalację sterowania instalacją oddymiania należy wykonać kablem HDGS PH90 2x1,5mm^2.

Celem umożliwienia bezpiecznej ewakuacji w przypadku pożaru zaprojektowano system różnicowania ciśnienia na klatkach schodowych ewakuacyjnych zlokalizowanych po obu stronach budynku. System ma za zadanie utrzymanie czystego powietrzna na klatkach schodowych poprzez niedopuszczenie do wpłynięcia dymu z korytarzy. W przypadku wystąpienia pożaru w obiekcie system będzie utrzymywał nadciśnienie na klatce schodowej zapobiegając zadymieniu klatki. Układ uruchamiany jest po przyjściu sygnału o pożarze z systemu SAP zamontowanego na obiekcie. Najpierw otwarta zostaje klapa (odpowiednio przepustnica wielopłaszczyznowa) po stronie ssawnej wentylatora mająca za zadanie odcięcie układu od warunków atmosferycznych w trybie czuwania. Następnie z kilkusekundową zwłoką staruje wentylator.

Instalację sterowania instalacją oddymiania należy wykonać kablem HDGS PH90 2x1,5mm^2.

Sterowanie kontrolą dostępu

Zwolnienie kontroli dostępu jest ściśle powiązane z ewakuacją zagrożonej strefy Sterowanie systemem kontroli dostępu odbywa się poprzez otwarcie obwodu zasilającego rygle kontroli dostępu. Moduły SSP sterujące kontrolą dostępu zostały zlokalizowane w pobliżu odpowiednich kontrolerów.

Instalację sterowania kontrolą dostępu należy wykonać kablem YnTKSYekw 1x2x0,8mm.

Monitoring zewnętrznych zasilaczy buforowych

Do analizy przyjęto zasilacze ZSP 135D o wydajności prądowej 2A przeznaczone do zasilania centralki systemu zasysającego wyposażone są w układy buforowanego ładowania akumulatorów oraz w układy kontrolujące poprawne działanie poszczególnych elementów. Wszelkie uszkodzenia (łącznie z brakiem zasilania sieciowego) sygnalizowane są świecącą się diodą LED oraz wysterowaniem dedykowanego przekaźnika.

SSP będzie monitorował sygnał uszkodzenia zbiorczego oraz informację o braku zasilania sieciowego zasilacza.

Instalację monitorowania zasilaczy ZSP należy wykonać kablem YnTKSYekw 1x2x0,8mm

Lista modułów

Lista modułów przedstawia identyfikacje modułów kontrolno-sterujących które zajmują się uruchamianiem i monitorowaniem poszczególnymi urządzeniami automatyki pożarowej. Na podstawie listy modułów i poszczególnych grup dozorowych czujek i ręcznych ostrzegaczy pożarowych należy na etapie wykonawstwa opracować w konsultacji z rzeczoznawcą ds. zabezpieczeń przeciwpożarowych matryce sterowań

Lista modułów

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
B3-REL16	nd	wy:1	1	DSO linia 1		
	nd	wy:2	2	DSO linia 2		
	nd	wy:3	3	DSO linia 3		
	nd	wy:4	4	DSO linia 4		
	nd	wy:5	5	DSO linia 5		
	nd	wy:6	6	DSO linia 6		
	nd	wy:7	7	DSO linia 7		
	nd	wy:8	8	DSO linia 8		
	nd	wy:9	9	DSO linia 9		
	nd	wy:10	10	DSO linia 10		
	nd	wy:11	11	DSO linia 11		
	nd	wy:12	12	DSO linia 12		
	nd	wy:13	13	REZEWA DO UTA		
	nd	wy:14	14	REZEWA DO UTA		
	nd	wy:15	15	REZEWA DO UTA		
	nd	wy:16	16	REZEWA DO UTA		
B5-BAF	nd	we:1	1	DSO uterka zbiorcza		
	nd	we:2	2	REZERWA		
BX-OI3	2:23	we:1				
		we:2				
		we:3				
		wy:1	100	Sterowanie KD	zwolnienie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	2:33	we:1				
		we:2				
		we:3				
		wy:1	101	Drzwi rozsuwane	zwolnienie	
BX-OI3	2:49	we:1				
		we:2				
		we:3				
		wy:1	102	Sterowanie KD	zwolnienie	
BX-OI3	2:70	we:1				
		we:2				
		we:3				
		wy:1	103	drzwi rozsuwane	zwolnienie	
BX-OI3	2:109	we:1	100	Nadciśnienie klatki schodowej	potwierdzenie	zadziałania
		we:2	101	Nadciśnienie klatki schodowej	usterka	ogólna
		we:3				
		wy:1	104	Nadciśnienie klatki schodowej	zadziałanie	
BX-O2I4	2:111	we:1	102	Klapy PPOŻ	potwierdzenie	
		we:2	103	Klapy PPOŻ	potwierdzenie	
		we:3	104	Klapy PPOŻ	potwierdzenie	
		we:4	105	Klapy PPOŻ	potwierdzenie	
		wy:1	105	Klapy PPOŻ	zamknięcie	
		wy:2	106	Klapy PPOŻ	zamknięcie	
BX-O2I4	2:112	we:1	106	Klapy PPOŻ	potwierdzenie	
		we:2	107	Klapy PPOŻ	potwierdzenie	
		we:3	108	Klapy PPOŻ	potwierdzenie	
		we:4	109	Klapy PPOŻ	potwierdzenie	
		wy:1	107	Klapy PPOŻ	zamknięcie	
		wy:2	108	Klapy PPOŻ	zamknięcie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-O2I4	2:113	we:1	110	Klapy PPOŻ	potwierdzenie	
		we:2	111	Klapy PPOŻ	potwierdzenie	
		we:3	112	Klapy PPOŻ	potwierdzenie	
		we:4	113	Klapy PPOŻ	potwierdzenie	
		wy:1	109	Klapy PPOŻ	zamknięcie	
		wy:2	110	Klapy PPOŻ	zamknięcie	
BX-O2I4	2:114	we:1	114	Klapy PPOŻ	potwierdzenie	
		we:2	115	Klapy PPOŻ	potwierdzenie	
		we:3	116	Klapy PPOŻ	potwierdzenie	
		we:4	117	Klapy PPOŻ	potwierdzenie	
		wy:1	111	Klapy PPOŻ	zamknięcie	
		wy:2	112	Klapy PPOŻ	zamknięcie	
BX-OI3	2:124	we:1				
		we:2				
		we:3				
		wy:1	113	Drzwi rozsuwane	zwolnienie	
BX-OI3	2:127	we:1				
		we:2				
		we:3				
		wy:1	114	Drzwi rozsuwane	zwolnienie	
BX-OI3	3:31	we:1				
		we:2				
		we:3				
		wy:1	115	Drzwi rozsuwane	zwolnienie	
BX-OI3	3:42	we:1				
		we:2				
		we:3				
		wy:1	116	Drzwi rozsuwane	zwolnienie	
BX-OI3	3:59	we:1				
		we:2				
		we:3				
		wy:1	117	Sterowanie KD	zwolnienie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	3:61	we:1	118	sterowanie systemem nadciśnienia klatki schodowej	potwierdzenie	zadziałania
		we:2	119	sterowanie systemem nadciśnienia klatki schodowej	usterka	ogólna
		we:3				
		wy:1	118	sterowanie systemem nadciśnienia klatki schodowej	zadziałanie	
BX-OI3	3:79	we:1				
		we:2				
		we:3				
		wy:1	119	Drzwi rozsuwane	zwolnienie	
BX-OI3	3:97	we:1				
		we:2				
		we:3				
		wy:1	120	Drzwi rozsuwane	zwolnienie	
BX-OI3	4:2	we:1				
		we:2				
		we:3				
		wy:1	201	Sterowanie KD	zwolnienie	
BX-O2I4	4:33	we:1	201	Klapy PPOŻ	potwierdzenie	
		we:2	202	Klapy PPOŻ	potwierdzenie	
		we:3	203	Klapy PPOŻ	potwierdzenie	
		we:4	204	Klapy PPOŻ	potwierdzenie	
		wy:1	202	Klapy PPOŻ	zamknięcie	
		wy:2	203	Klapy PPOŻ	zamknięcie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	4:40	we:1				
		we:2				
		we:3				
		wy:1	204	Sterowanie KD	zwolnienie	
BX-OI3	4:41	we:1				
		we:2				
		we:3				
		wy:1	205	Sterowanie KD	zwolnienie	
BX-OI3	4:43	we:1	205	Klapy PPOŻ	potwierdzenie	
		we:2	206	Klapy PPOŻ	potwierdzenie	
		we:3				
		wy:1	206	Klapy PPOŻ	zamknięcie	
BX-OI3	4:44	we:1	208	Klapy PPOŻ	potwierdzenie	
		we:2	209	Klapy PPOŻ	potwierdzenie	
		we:3				
		wy:1	207	Klapy PPOŻ	zamknięcie	
BX-OI3	4:66	we:1	211	sterowanie systemem nadciśnienia klatki schodowej	potwierdzenie	zadziałania
		we:2	212	sterowanie systemem nadciśnienia klatki schodowej	usterka	ogólna
		we:3				
		wy:1	208	sterowanie systemem nadciśnienia klatki schodowej	zadziałanie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	4:115	we:1	213	Zasilacz PPOŻ	uszkodzenie ogólne	
		we:2	214	Zasilacz PPOŻ	brak zasilania	siecowego
		we:3				
		wy:1				
BX-O2I4	4:117	we:1	215	Klapy PPOŻ	potwierdzenie	
		we:2	216	Klapy PPOŻ	potwierdzenie	
		we:3	217	Klapy PPOŻ	potwierdzenie	
		we:4	218	Klapy PPOŻ	potwierdzenie	
		wy:1	209	Klapy PPOŻ	zamknięcie	
		wy:2	210	Klapy PPOŻ	zamknięcie	
BX-O2I4	4:118	we:1	219	Klapy PPOŻ	potwierdzenie	
		we:2	220	Klapy PPOŻ	potwierdzenie	
		we:3	221	Klapy PPOŻ	potwierdzenie	
		we:4	222	Klapy PPOŻ	potwierdzenie	
		wy:1	211	Klapy PPOŻ	zamknięcie	
		wy:2	212	Klapy PPOŻ	zamknięcie	
BX-O2I4	4:119	we:1	223	Klapy PPOŻ	potwierdzenie	
		we:2	224	Klapy PPOŻ	potwierdzenie	
		we:3	225	Klapy PPOŻ	potwierdzenie	
		we:4	226	Klapy PPOŻ	potwierdzenie	
		wy:1	213	Klapy PPOŻ	zamknięcie	
		wy:2	214	Klapy PPOŻ	zamknięcie	
BX-O2I4	4:120	we:1	227	Klapy PPOŻ	potwierdzenie	
		we:2	228	Klapy PPOŻ	potwierdzenie	
		we:3	229	Klapy PPOŻ	potwierdzenie	
		we:4	230	Klapy PPOŻ	potwierdzenie	
		wy:1	215	Klapy PPOŻ	zamknięcie	
		wy:2	216	Klapy PPOŻ	zamknięcie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	5:44	we:1				
		we:2				
		we:3				
		wy:1	217	Sterowanie KD	zwolnienie	
BX-OI3	5:45	we:1				
		we:2				
		we:3				
		wy:1	218	Sterowanie KD	zwolnienie	
BX-OI3	5:46	we:1				
		we:2				
		we:3				
		wy:1	219	Sterowanie KD	zwolnienie	
BX-OI3	5:47	we:1				
		we:2				
		we:3				
		wy:1	220	Sterowanie KD	zwolnienie	
BX-OI3	5:57	we:1				
		we:2				
		we:3				
		wy:1	221	Sterowanie KD	zwolnienie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	5:69	we:1	231	sterowanie żaluzjami nadciśnienia klatki schodowej	potwierdzenie	zadziałania
		we:2	232	sterowanie żaluzjami nadciśnienia klatki schodowej	usterka	ogólna
		we:3				
		wy:1	222	sterowanie żaluzjami nadciśnienia klatki schodowej	zadziałanie	
BX-OI3	6:1	we:1	301	REZERWA		
		we:2	302	REZERWA		
		we:3				
		wy:1	301	Centrala wentylacyjna	wyłączenie	
BX-OI3	6:3	we:1	303	REZERWA		
		we:2	304	REZERWA		
		we:3				
		wy:1	302	Centrala wentylacyjna	wyłączenie	
BX-OI3	6:13	we:1	305	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	306	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	303	Centrala oddymiająca	zadziałanie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	6:15	we:1	307	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	308	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	304	Centrala oddymiająca	zadziałanie	
BX-OI3	6:28	we:1	309	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	310	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	305	Centrala oddymiająca	zadziałanie	
BX-OI3	6:29	we:1	311	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	312	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	306	Centrala oddymiająca	zadziałanie	
BX-OI3	6:31	we:1	313	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	314	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	307	Centrala oddymiająca	zadziałanie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	6:32	we:1	315	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	316	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	308	Centrala oddymiająca	zadziałanie	
BX-OI3	6:50	we:1	317	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	318	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	309	Centrala oddymiająca	zadziałanie	
BX-OI3	6:52	we:1	319	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	320	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	310	Centrala oddymiająca	zadziałanie	
BX-OI3	6:54	we:1	321	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	322	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	311	Centrala oddymiająca	zadziałanie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	6:55	we:1	323	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	324	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	312	Centrala oddymiająca	zadziałanie	
BX-OI3	6:63	we:1	325	REZERWA		
		we:2	326	REZERWA		
		we:3				
		wy:1	313	Centrala wentylacyjna	wyłączenie	
BX-OI3	6:68	we:1	327	Kurtyna dymowa	potwierdzenie	zadziałania
		we:2	328	Kurtyna dymowa	usterka	ogólna
		we:3				
		wy:1	314	Kurtyna dymowa	zadziałanie	
BX-OI3	6:69	we:1	329	Kurtyna dymowa	potwierdzenie	zadziałania
		we:2	330	Kurtyna dymowa	usterka	ogólna
		we:3				
		wy:1	315	Kurtyna dymowa	zadziałanie	
BX-OI3	6:71	we:1	331	Centrala oddymiająca	potwierdzenie	zadziałania
		we:2	332	Centrala oddymiająca	usterka	ogólna
		we:3				
		wy:1	316	Centrala oddymiająca	zadziałanie	

Element	Adres fizyczny	Typ	Adres logiczny	Opis 1	Opis 2	Opis 3
BX-OI3	6:77	we:1	333	REZERWA		
		we:2	334	REZERWA		
		we:3				
		wy:1	317	Centrala wentylacyjna	wyłączenie	
BX-OI3	6:78	we:1	335	REZERWA		
		we:2	336	REZERWA		
		we:3				
		wy:1	318	Centrala wentylacyjna	wyłączenie	

Wykonanie systemu sygnalizacji pożarowej

Montaż instalacji

System sygnalizacji pożarowej stanowi niezależną wydzieloną instalację bezpieczeństwa. W systemie należy przewidzieć zasilanie podstawowe z wydzielonego obwodu zasilania gwarantowanego sprzed wyłącznika głównego prądu. Do tego wydzielonego obwodu nie można podłączać żadnych innych odbiorów energii elektrycznej. Instalację linii dozorowych należy wykonać w teletechnicznych korytach kablowych lub w rurkach PCV montowanych do stropu.

Linie dozorowe należy wykonać przewodem ekranowanym YnTKSYekw 1x2x0,8mm w powłoce koloru czerwonego. Dopuszcza się zmianę kolejności elementów w pętli, jednakże każda zmiana winna być zaznaczona na dokumentacji powykonawczej.

Przy instalowaniu elementów należy uwzględnić wytyczne do projektowania określające sposób montażu (tzn. aby czujki znajdowały się w odległości większej niż 0,5m od ścian, belek stropowych, podciągów i innych przegród pionowych oraz kratek wyciągowych wentylacji oraz w odległości 1,5m od kratek wentylacyjnych nawiewnych). Czujki dozorujące przestrzeń międzystropową montować pośrodku pól utworzonych przez podciągi, ściany czy dukty wentylacyjne lub możliwe blisko urządzeń zakwalifikowanych jako stanowiące ewentualne zagrożenie pożarowe (rozdzielnie sterujące, itp.) W przypadku sufitów nierozbieralnych należy przewidzieć otwory rewizyjne umożliwiające dostęp serwisowy do czujki. Zarówno na sufitach nierozbieralnych jak i na modułach rozbieranego sufitu podwieszanego stanowiącego dostęp do czujki międzystropowej należy zamontować wskaźnik zadziałania w sposób jednoznacznie wskazujący której czujki międzystropowej dotyczy.

Czujki montowane do betonowej konstrukcji budynku należy zamontować do stropu przy pomocy kołków. Czujki montowane do konstrukcji stalowej przy pomocy gwoździ wbijanych do betonu. Czujki montowane na rozbieranych stropach podwieszanych oraz do stropów wykonanych z pełnej płyty kartonowo-gipsowej należy zamontować przy pomocy kołków właściwych do płyt gipsowych zaś kable doprowadzać przez płytę bezpośrednio od góry do gniazda czujki.

Ręczne ostrzegacze pożarowe montować na wysokości ok. 1,2-1,6m od poziomu podłogi. Dojścia do przycisków ROP wykonać podtynkowo lub w rurkach PCV. W trakcie eksploatacji należy zwrócić uwagę by ROPy nie zostały zasłonięte w związku z późniejszą aranżacją pomieszczeń przez drzwi, meble itp.

Przebiegi tras kablowych przedstawiono na rysunkach rzutów budynku. Wszystkie elementy systemu należy oznakować zgodnie z projektem.

Zasilanie CSP należy wykonać kablem z wydzielonego pola rozdzielni pożarowej. W pobliżu centralki należy umieścić instrukcję obsługi centrali, książkę kontroli systemu, instrukcję postępowania w przypadku alarmów pożarowych i uszkodzeniowych oraz dokumentację systemu.

Montaż urządzeń należy wykonać w oparciu o fabryczną dokumentację techniczno-ruchową producenta urządzeń. SSP należy regularnie poddawać przeglądom konserwacyjnym zgodnie z wytycznymi PKN-CEN/TS 54-14 CNBOP i zaleceniami producenta systemu.

Wytyczne dla inwestora i użytkownika

W pomieszczeniu, w którym znajdzie się dozór przy centrali użytkownik powinien zapewnić:

- instrukcję obsługi centrali
- książkę eksploatacji systemu, do której należy wpisywać: okresowe kontrole instalacji i urządzeń, dokonane naprawy, zmiany i uzupełnienia instalacji, wszystkie alarmy z podaniem daty i godziny ich wystąpienia, wyłączenia czujek, stref, linii
- dokumentację techniczną systemu zawierającą opis jego działania, sposób zasilania, umożliwiającą łatwą identyfikację linii dozorowych, stref, nadzorowanych pomieszczeń, rodzajów czujek

W czasie odbioru Wykonawca SSP powinien przekazać Inwestorowi następujące dokumenty:

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

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

sprawdzić codziennie:

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

sprawdzić raz w miesiącu:

- prawidłowe działanie wszystkich wskaźników (poprzez test wskaźników),
- wystarczający zapas papieru w drukarce,

zapewnić raz na kwartał aby osoby kompetentne przeprowadziły kontrolę/testy:

- zadziałania co najmniej jednej czujki i jednego ROP-a w każdej grupie dozorowej
- prawidłowego wyświetlania komunikatów o pobudzonych elementach oraz emitowania sygnałów optycznych i akustycznych przez centralę,
- sprawdzające prawidłowe sterowanie i monitorowanie wszystkich elementów współpracujących z systemem sygnalizacji pożarowej,
- czy nie nastąpiły zmiany budowlane, architektoniczne, przeznaczenia pomieszczeń, bądź umeblowania mogące mieć wpływ na poprawność rozmieszczenia czujek, ROPów i sygnalizatorów akustycznych,

zapewnić aby raz w roku przeszkolony specjalista przeprowadził czynności:

- zalecane dla obsługi codziennej, miesięcznej i kwartalnej,
- sprawdził każdą czujkę na poprawność działania przez pobudzenie (dopuszcza się raz na kwartał przetestowanie kolejnych 25% wszystkich czujek)
- sprawdził wzrokowo, czy wszystkie połączenia kablowe i aparatura są sprawne, nieuszkodzone i odpowiednio zabezpieczone
- sprawdził stan wszystkich akumulatorów.

Przeglądy okresowe (roczne, ewentualnie kwartalne) powinny być wykonywane przez wyspecjalizowany personel posiadający odpowiednie uprawnienia i wiedzę techniczną. System sygnalizacji pożarowej oparty na urządzeniach firmy Schrack Seconet powinien być konserwowany przez autoryzowanego partnera firmy Schrack Seconet.

Montaż instalacji uwagi dodatkowe

Montaż wykonywać zgodnie z obowiązującymi w kraju normami i przepisami.

- Celem uniknięcia kolizji zaleca się przeprowadzenie montażu instalacji SAP w koordynacji z innymi branżami.
- Sposób wykonywania połączeń między elementami linii zostanie podany w projekcie wykonawczym. Połączenia wykonać kablem typu YnTKSY 2x1 lub 2x0.8 wciąganym do rur winidurowych fi18 mocowanych do sufitu lub układanych w istniejących korytach przeznaczonych dla instalacji teletechnicznych lub układanych poddtynkowo. Obwody linii wykonawczych gdzie wymagane jest zapewnienie podczas pożaru zasilania wykonać kablem o odpowiedniej odporności ogniowej. Przewody układać na uchwytach niepalnych E30/E90 posiadających dopuszczenie wymagane prawem. Sposób mocowania musi być zgodny z certyfikatem lub aprobatą.
- Obwody sygnalizatorów akustycznych na kondygnacjach łączyć tak, by były dozorowane przez centralę sygnalizacji pożaru.

- Przejścia przez ściany i stropy będące elementami wydzieleń pożarowych należy uszczelnić za pomocą odpowiednich mas uszczelniających.
- Czujki instalować zawsze bezpośrednio na stropie.
- Podczas montażu sprawdzać numerację i nazwy pomieszczeń. Dane te są niezbędne do wykonania opisu tekstowego w centrali. Nazwy pomieszczeń, ich numerację oraz nazwy stref określać w porozumieniu z Zamawiającym (Użytkownikiem).
- W przypadkach kolizji lub zbliżeń zachować odległość 50 cm czujek od ścian, podciągów, przewodów wentylacyjnych (o ile przebiegają one w odległości mniejszej niż 15 cm od stropu), opraw świetlnych itp.
- Zachować odległość min. 1,5 m od kratek wentylacyjnych nawiewu i wywiewu.
- Zachować odległość min. 30 cm przewodów instalacji SAP od innych przewodów i kabli elektrycznych.
- Początki i końce linii dozorowych prowadzone w częściach pionowych instalacji prowadzić w osobnych rurach, przy czym dopuszcza się stosowanie wspólnej rury dla „początków" i wspólnej rury dla „końców" linii pętlowych.
- Ręczne ostrzegacze pożaru instalować na wysokości 1,2-1,6 m od podłogi.
- Centralę sygnalizacji pożaru zainstalować na wysokości umożliwiającej łatwy odczyt informacji z jej pola odczytowego.

Zasilanie instalacji

Projekt zakłada zasilanie podstawowe 230 V pr. zm. z wydzielonego pola rozdzielni głównej obiektu, z przed wyłącznika głównego prądu.

UWAGA! Do obwodu zasilającego SAP nie wolno przyłączać innych odbiorników energii elektrycznej. Pole podłączenia zasilania oznaczyć napisem „CENTRALA SAP".

Połączenie kablowe wykonać jako nierozłączne. Stosować odpowiednie zasady ochrony przeciwporażeniowej.

Projekt przewiduje zastosowanie centralki SAP wyposażonej w zasilanie awaryjne zapewniające pracę przez 72 h dla stanu czuwania i 0.5 h dla stanu alarmu.

Wytyczne dla branży elektrycznej

Rozdzielnie zasilające siłowniki klap przeciwpożarowych odcinających muszą być wyposażone w styczniki (z cewkami na 24V) umożliwiające wyłączenie zasilania przez moduł sterujący znajdujący się na pętli systemu SAP.

Uwagi ogólne

- Zaprojektowane instalacje muszą być wykonane zgodnie z postanowieniami aktualnie obowiązujących norm, przepisów i wytycznych oraz zaleceniami producentów poszczególnych systemów;
- Sposób układania kabli teletechnicznych uzależnić od innych instalacji elektrycznych w obiekcie. Kable powinny być chronione przed uszkodzeniami poprzez ułożenie ich w wydzielonym korytku lub w rurach ochronnych PCV. Przy układaniu kabli należy zachować jak największe odległości od innych instalacji elektrycznych, dla instalacji o napięciu 230 V i wyższym (min. 30 cm).
- Ekrany kabli i obudowy urządzeń uziemiać zgodnie z wymaganiami producenta w celu zapewnienia odpowiedniej ochrony tj. zmniejszenia pętli sprzężeń, zakłóceń, przesłuchów itp.

Zestawienie materiałów

W projekccie analizowano i do obliczeń przyjęto elementy systemu Schrack Seconet. Można zastosowac system innego producenta zgodny z przywołanymi przepisami i ormami oraz o parametrach technicznych nie gorszych niż przyjęty do obliczeń.

LP	Element	Typ	Producent	Ilość
1	B5-Redundantna centrala z drzwiami pełnymi + zasilacz B5-PSU (7A) lub równoważne	B5-SCU	Schrack Seconet	1
2	B5-DXI2 Redundantna karta linii pętlowych x-line, do 500 elementów lub równoważne	B5-DXI2	Schrack Seconet	3
3	Redundantna karta sieciowa IP B5-NET2-485 lub równoważne	B5-NET2-485	Schrack Seconet	1
4	Adapter komunikacyjny RJ45 lub równoważne	KUP 9RJ45	Schrack Seconet	2
5	B3-REL16 Karta przekaźnikowa lub równoważne	B3-REL16	Schrack Seconet	1
6	Wtyczki REL16 z wyjściami kątowymi lub równoważnae	ST-SET REL16 W	Schrack Seconet	1
7	B5-BAF Redundantna karta sterująca (2we; 2wy 1,5A), interfejs MMI-Bus lub równoważne	B5-BAF	Schrack Seconet	1
8	Karta pamięci SD 512 MB lub równoważne	SD-CARD	Schrack Seconet	1
9	Maskownica wolnych slotów Integral IP lub równoważne	B3 BLIND	Schrack Seconet	5
10	Akumulator 12 V 44 Ah lub równoważne	AKKU 44	Schrack Seconet	2
11	B5 Redundantne zewnętrzne pole obsługi MAP PL z drukarką lub równoważne	B5-MMI-CPP-PL	Schrack Seconet	1
12	Pakiet oprogramowania gateway OPC_Schrack lub równoważne	OPC_Schrack	Schrack Seconet	1
13	CUBUS MTD 533X interaktywna czujka wielokryteryjna (TF1-TF9) lub równoważne	CUBUS MTD 533X	Schrack Seconet	469
14	CUBUS MTD 533X (TF1-TF9) z lakierowaną płytką elektr lub równoważne	CUBUS MTD533X CP	Schrack Seconet	25

LP	Element	Typ	Producent	Ilość
15	Gniazdo standardowe USB 501-1 lub równoważne	USB 501-1	Schrack Seconet	469
16	Gniazdo do pomieszczeń wilgotnych USB 501-3 IP54 lub równoważne	USB 501-3	Schrack Seconet	25
17	Wskaźnik zadziałania BX-UPI, elektronika lub równoważne	BX-UPI	Schrack Seconet	168
18	Obudowa wskaźnika zadziałania lub równoważne	PIG	Schrack Seconet	168
19	Przycisk pożarowy MCP545X-1R-PL natynkowy, IP24 lub równoważne	MCP545X-1R-PL	Schrack Seconet	38
20	Przycisk pożarowy MCP535X-1 kolor czerwony (IP 52) lub równoważne	MCP 535X-1	Schrack Seconet	5
21	Szyld opisowy dla MCP535X lub równoważne	MCP 535 AK	Schrack Seconet	5
22	Moduł wejścia / wyjścia BX-OI3, 2we + optozłącze, 1wy (60W) failsafe lub równoważne	BX-OI3	Schrack Seconet	44
23	Moduł wejścia / wyjścia BX-O2I4, 4we, 2wy (60W) failsafe lub równoważne	BX-O2I4	Schrack Seconet	9
24	Obudowa modułu IP66 lub równoważne	GEH MOD IP66	Schrack Seconet	44
25	Obudowa modułu IP66 dla BX-REL4/BX-O2I4	GEH MOD2 IP66	Schrack Seconet	9
26	Nypel wielostopniowy M 20 lub równoważne	MM SN M20	Schrack Seconet	292
27	System zasysający ASD 535-2 (bez detektorów) lub równoważne	ASD 535-2	Schrack Seconet	1
28	Detektor dymu dla ASD 535, SSD 535-2 (0,1 %/m) lub równoważne	SSD 535-2	Schrack Seconet	2
29	Moduł pętlowy XLM 35 dla ASD 535 (1 szt./ASD) lub równoważne	XLM 35	Schrack Seconet	1

LP	Element	Typ	Producent	Ilość
30	Klej 1 kg lub równoważne	RAS KLG	Schrack Seconet	2
31	Środek do czyszczenia (1 litr) lub równoważne	RAS RNG	Schrack Seconet	2
32	PVC Rura d25/ długość 5 metrów (TU 25 PVC) lub równoważne	RAS R25	Schrack Seconet	20
33	PVC Łuk 90° d25 (BE 25 PVC) lub równoważne	RAS B9025	Schrack Seconet	10
34	PVC Trójnik d25 (TP 25 PVC) lub równoważne	RAS T25	Schrack Seconet	6
35	PVC Mufa d25 (SO 25 PVC) lub równoważne	RAS M25	Schrack Seconet	22
36	PVC Zatyczka d25 (EC 25 PVC) lub równoważne	RAS E25	Schrack Seconet	8
37	PVC Klips d25/2.0mm (CLIP 2.0 PA) lub równoważne	RAS CLP 2520	Schrack Seconet	3
38	PVC Klips d25/2.5mm (CLIP 2.5 PA) lub równoważne	RAS CLP 2525	Schrack Seconet	10
39	PVC Klips d25/3.0mm (CLIP 3.0 PA) lub równoważne	RAS CLP 2530	Schrack Seconet	4
40	PVC Klips d25/3.5mm (CLIP 3.5 PA) lub równoważne	RAS CLP 2535	Schrack Seconet	1
41	Uchwyt montażowy IKS d25 (100 szt) lub równoważne	RAS BSIKS25	Schrack Seconet	2
42	Filtr przeciwpyłowy DFU 535L lub równoważne	DFU 535L	Schrack Seconet	2
43	Zasilacz pożarowy do systemu ASD lub równoważne	ZSP135-DR-2A-1	Merawex	1
44	Przewód do pętli dozorowej lub równoważne	YnTKSYekw 1x2x0,8mm	Technokabel	6000

LP	Element	Typ	Producent	Ilość
45	Przewód zasilający do zewnętrznego panelu sterowania lub równoważne	HDGS 2x1,5mm2 PH90	Technokabel	20
46	Przewód magistralny do zewnętrznego panlu sterowania lub równoważne	HTKSHekw 1x2x0,8mm PH90	Technokabel	20
47	Rury PCV fi 18 lub równoważne	typowe	typowe	2000
48	Elementy drobne (kołki, uchwyty itp..) lub równoważne	komplet	typowe	1

Można zastosować elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż przyjęte w projekcie. Zmiana elementów systemu na inny niz zaprojektowane wymaga ponownego wykonania obliczeń prądowych i kalkulacji pętli.

Sterowanie oddymianiem

Projekt zawiera sterowanie urządzeniami oddymiającymi. Oddymianie głównej części budynku zostało zaprojektowane na podstawie symulacji komputerowych CFD przeprowadzonych na trójwymiarowym modelu obiektu, uwzględniającym jego podstawowe parametry techniczne, takie jak geometria, podział na strefy pożarowe i dymowe, lokalizacja otworów wentylacji naturalnej i mechanicznej oraz rozmieszczenie i długości kurtyn dymowych. Analizie poddano części obiektu, w których zastosowano systemy grawitacyjnej wentylacji oddymiającej, obejmujące 3 strefy dymowe zaznaczone na rysunku. Określony został przewidywany czas ewakuacji użytkowników obiektu w przypadku wystąpienia pożaru oraz czas, po którym na drogach ewakuacyjnych nastąpi przekroczenie dopuszczalnych wartości analizowanych parametrów pożaru. Dokonano oceny wpływu tych parametrów na skuteczną ewakuację. Poniżej zostały przedstawione założenia przyjęte do analiz w zakresie geometrii obiektu i zastosowanych w nim systemów zabezpieczeń przeciwpożarowych oraz analizowanych scenariuszy pożarowych:

a. Analizowany obszar obiektu obejmuje trzy strefy dymowe Terminalu Lotniczego w Szymanach: SD „A”, SD „B”, SD „C” oddymianych grawitacyjnie, obejmujących przyziemie oraz antresolę,
b. W analizowanym obszarze obiektu występują ruchome lub stałe kurtyny dymowe, co najmniej klasy D60 wg PN-EN 12101:1 [8], których dolna krawędź znajduje się w czasie pożaru na odpowiedniej wysokości od posadzki,
c. Pomieszczenia antresol, oddzielone są od przestrzeni przyziemia ścianami EI15,
d. W analizowanym obiekcie nie występuje instalacja tryskaczowa,
e. W analizowanym obiekcie zastosowany jest dźwiękowy systemu ostrzegawczy.
f. Klatki schodowe są wydzielone pożarowo od pozostałej części budynku oraz zabezpieczone przed zadymieniem za pomocą systemu nawiewu powietrza zapewniającego nadciśnienie.
g. Oddymianie realizowane jest za pomocą klap dymowych zlokalizowanych w świetlikach dachu, o powierzchni czynnej 20m dla każdej strefy dymowej,
h. Powietrze uzupełniające dla potrzeb oddymiania jest dostarczane przez otwarte drzwi zewnętrzne do obiektu (NN), o łącznej powierzchni czynnej 23,7m^2,
i. Wentylacja oddymiająca jest uruchamiana w danej strefie dymowej natychmiast po zadziałaniu w niej 2 czujek. Następuje wówczas otwarcie klap dymowych oraz otworów

wszystkich napływu powietrza uzupełniającego. Równocześnie zostaje wyłączona wentylacja bytowa w całej analizowanej strefie pożarowej i opadają rozwijane kurtyny dymowe wokół strefy dymowej objętej pożarem,

j. Zakłada się, iż czas dojazdu jednostek ratowniczo gaśniczych na miejsce zdarzenia nie przekroczy 3 min. (obecność Lotniskowej Służby Ratowniczo-Gaśniczej). Uwzględniając dodatkowo czas 60 s przewidziany na wykrycie pożaru i przekazanie informacji o zdarzeniu oraz 60 s na rozpoczęcie działań gaśniczych, przyjęto, iż maksymalny czas rozwoju pożaru do rozpoczęcia działań gaśniczych nie będzie przekraczał 5 min.

Na podstawie powyższych założeń przyjęto, iż maksymalna moc pożaru (rozwijającego się z założoną szybkością „pożaru szybkiego") nie przekroczy 5000 kW, co stanowy podstawę do przeprowadzonych wstępnych obliczeń powierzchni czynnej klap.

Opis sterowania oddymianiem

Obszar obiektu obejmuje trzy strefy dymowe: SD „A", SD „B", SD „C" oddymianych grawitacyjnie, obejmujących przyziemie oraz antresolę. W analizowanym obszarze obiektu występują ruchome (między osiami 10d -11,b w osi Ba) i stałe kurtyny dymowe. Kurtyna dymowa sterowana jest modułem sterującym systemu sygnalizacji pożaru. Oddymianie realizowane jest za pomocą klap dymowych zlokalizowanych w świetlikach dachu, o powierzchni czynnej 20 m^2 dla każdej strefy dymowej. Dobór powierzchni czynnej oddymiania na podstawie symulacji komputerowej w projekcie architektonicznym.

Każde pasmo świetlików składa się z 6 klap oddymiających dwuskrzydłowych. Każda klapa wyposażona jest w zespół dwóch siłowników (dobór w projekcie architektonicznym) o poborze prądu 4A na każdą klapę.

Łączny pobór prądu dla jednego pasma świetlików wynosi 24 A.

Dla każdego pasma świetlików zaprojektowano centralę oddymiającą o wydajności prądowej 24A. W projekcie do analizy i obliczeń przyjęto centralę AFG-2004/24A 3L3G lub równoważne. Centrale są sterowane i monitorowane za pomocą modułów kontrolno-sterujących systemu sygnalizacji pożaru. Dla każdej centrali przewidziano jeden moduł.

W każdej strefie zaprojektowano po 4 pasma świetlików z klapami oddymiającymi

Nawiew powietrza zapewnia otwarcie drzwi wejściowych do budynku. Dobór powierzchni napowietrzającej na podstawie symulacji komputerowej w projekcie architektonicznym.

Otwarcie drzwi następuje na podstawie sygnału sterującego (styk bezpotencjałowy) z modułu systemu sygnalizacji pożaru za pomocą siłowników drzwiowych. Dobór siłowników w projekcie architektonicznym. Do napowietrzania wykorzystanych jest 7 otworów drzwiowych.

Opis sterowania przewietrzaniem

Zaprojektowano funkcje przewietrzania z wykorzystaniem klap oddymiający w świetlikach dachowych oraz kompensacją powietrza przez oka uchylne na szczytach budynku.
Sterowanie otwarciem w funkcji przewietrzania przez BMS.
Na obu szczytach budynku między osiami Ad - A na wysokości stropu I-go piętra zaprojektowano okna uchylne po 5 szt. z każdej strony. Każde z tych okien zaopatrzone jest w siłownik poborze prądu 4A. Dobór siłowników w projekcie architektonicznym. Uchylenie okien ma zapewnić napływ powietrza kompensacyjnego w funkcji przewietrzania. Okna te nie są przewidziane do wykorzystania w funkcji oddymiania. Dla otwarcia okien kompensacyjnych zaprojektowano centralki oddymiające po jednej dla każdej ze stron budynku.
Łączny pobór prądu dla zespołu okien dla każdej strony budynku wynosi 20A. Dla każdego zespołu okien zaprojektowano centralę oddymiającą o wydajności prądowej 24A. W projekcie do analizy i obliczeń przyjęto centralę AFG-2004/24A 3L3G. Centrale są sterowane i monitorowane przez BMS. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.
BMS umożliwia sterowanie funkcja przewietrzania "ręcznego" lub z możliwością zaprogramowania funkcji czasowych lub za pomocą analizy temperatury wewnątrz i na zewnątrz obiektu. Dla zabezpieczenia klap oddymiających BMS pobiera również sygnał centralki pogodowej i w razie wystąpienia opadów deszczu lub zbyt silnego wiatru zamyka klapy oddymiające i okna. Zawsze funkcja odymiania jest nadrzędna nad każdą inna funkcją.

Zestawienie materiałów

nazwa	jm	ilość
Centrala oddymiająca AFG-2004 48A 1L6G (do otwierania klap oddymiających w funkcji oddymiania i przewietrzania) lub równoważne	szt.	12
centrala odymiająca AFG-2004/24A 3L3G (3x8A))do okien kompensujących przy funkcji przewietrzania) lub równoważne	szt.	2
centralka pogodowa CDW-02 lub równoważne	szt.	1
Kabel silikonowy HDGs PH90 2x2,5 300/500V drut lub równoważne	m	1800

Można zastosować elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż przyjęte w projekcie. Zmiana elementów systemu na inny niz zaprojektowane wymaga ponownego wykonania obliczeń prądowych i kalkulacji pętli.

Zapobieganie zadymieniu na klatkach chodowych

Celem umożliwienia bezpiecznej ewakuacji w przypadku pożaru zaprojektowano system różnicowania ciśnienia na klatkach schodowych ewakuacyjnych zlokalizowanych po obu stronach budynku. System ma za zadanie utrzymanie czystego powietrzna na klatkach schodowych poprzez niedopuszczenie do wpłynięcia dymu z korytarzy. W przypadku wystąpienia pożaru w obiekcie system będzie utrzymywał nadciśnienie na klatce schodowej zapobiegając zadymieniu klatki. System zaprojektowano w oparciu o PN-EN 12101-6:2007 Systemy kontroli rozprzestrzeniania się dymu i ciepła. Część 6: Wymagania techniczne dotyczące systemów różnicowania ciśnień. Zabezpieczenie przestrzeni chronionej (np. na klatce schodowej) realizowane jest poprzez wytworzenie w niej nadciśnienia 50Pa (+/-10%). Regulacja ciśnienia realizowana będzie poprzez nawiew do przestrzeni klatki schodowej odpowiednich ilości powietrza w zależności od przyjętego kryterium zgodnie z projektem i normą PN-EN 12101-6. Układ uruchamiany jest po przyjściu sygnału o pożarze z systemu SAP zamontowanego na obiekcie. Najpierw otwarta zostaje klapa (odpowiednio przepustnica wielopłaszczyznowa) po stronie ssawnej wentylatora mająca za zadanie odcięcie układu od warunków atmosferycznych w trybie czuwania. Następnie z kilkusekundową zwłoką staruje wentylator. W przypadku gdy wszystkie drzwi na klatce schodowej są zamknięte, wentylator pracuje z wydatkiem powietrza potrzebnym dla wytworzenia i stabilizacji nadciśnienia 50Pa (+/-10%) na całej wysokości klatki schodowej. Pomiar aktualnej wartości nadciśnienia w przestrzeni klatki schodowej odbywa się odpowiednio zmieniając prędkość obrotową wentylatora. W momencie otwarcia którykolwiek drzwi na klatce schodowej, wartość ciśnienia na klatce gwałtownie spada co powoduje natychmiastowe rozpędzenie wentylatora i zwiększenie ilości powietrza dostarczanego na klatkę do tej wymaganej przez kryterium otwartych drzwi. Jednocześnie należy pamiętać o zapewnieniu upustu dymu z kondygnacji objętej pożarem celem uzyskania wymaganej prędkości na drzwiach otwartych (np. poprzez otwarcie klapy ppoż na kanale służącym do upustu dymu). Podobnie wygląda praca układu dla spełnienia kryterium 10Pa wg. normy PN-EN 12101-6. Należy również pamiętać o konieczności stosowania samozamykaczy

we wszystkich drzwiach oddzielających przestrzeń chronioną. Montaż układu zabezpieczenia przed zadymieniem kończy się kalibracją i uruchomieniem układu przez serwis producenta po którym sporządzony zostaje protokół z pomiarów. Wytwarzanie nadciśnienia na klatce schodowej z wykorzystaniem falownika powoduje brak konieczności stosowania klapy nadmiarowo upustowej. Nadmiar powietrza dostający się z klatki schodowej na kondygnację przy otwartych drzwiach będzie usuwany przez żaluzję nad drzwiami na końcach korytarzy.

Obliczenia dla klatki zachodniej

Suma przeciekow	**0,07257**	**m2**	
Przecieki przez drzwi			
	ilosc	pow. nieszcz.	
Drzwi jednoskrzydl otw do przestrz o podw cisn	2	0,01	
Drzwi jednoskrzydl otw z przestrz o podw cisn	1	0,02	
Drzwi dwuskrzydl	0	0,03	
Ae_drzwi	**0,04**	**m2**	
Przecieki przez ściany wew			
szczelna		1,4E-05	
przeciętna		1,1E-04	
nieszczelna		3,5E-04	
A_ścian-wew	232	m2	
A_drzwi-wew	0	m2	
A_ścian netto-wew	232	m2	
Ae_ścian wew	**0,026**	**m2**	
Przecieki przez okna	ilosc	obwod	
rozwierane bez uszczeln	2	6,4	m
rozwierane z uszczeln	0	0	m
przesuwne	0	0	m
Ae_okien	**0,00320**	**m2**	
Przecieki przez stropy			
A_stropow	74,00	m2	
przeciętny	5,2E-05		
Ae_stropy	**0,004**	**m2**	
Przecieki przez ściany zew			
szczelna		7,0E-05	
przeciętna		2,1E-04	
nieszczelna		4,2E-04	
bardzo nieszczelna		1,3E-03	
A_ścian-zew	0	m2	
A_drzwi-zew	0	m2	
A_ścian netto-zew	0	m2	
Ae_ścian zew	**0,000**	**m2**	
Przecieki do szybu windy	Ilosc		Ae
Drzwi szybu windy w klatce schodowej	0		0
Drzwi szybu windy do innych pomieszczen	0		0
Otwor dla przewietrzania szybu windy	0	m2	
przecietna	0,00084		
Sciany szybu windy (z peknieciami w konstrukcji ale bez szczelin wokol okien i drzwi)	0	m2	0
Ogolna powierzchnia przeciekow do szybu windy	0,00000	m2	
Ogolna powierzchnia przeciekow z szybu windy	0,000	m2	
Powierzchnia nieszczelnosci dla szybu windy	**0,0000**	**m2**	

Klasa systemu	C

Predkosc powietrza na drzwiach otw [m/s]:	0,75
Drzwi zewnetrzne	zamkniete
Ilosc innych otwartych drzwi	0
Drzwi zewnetrzne dla kryterium nadcisnienia 10 Pa	otwarte
Ilosc innych drzwi otwartych dla kryterium nadcisnienia 10Pa	0

Kryterium różnicy ciśnienia

Wszystkie drzwi zamknięte

Qd	0,83*Ae*P^(1/R)	
Ae	0,0726	
P	50	
R	2	
Q50	0,43	m3/s
Q50	**1 533**	**m3/h**
wsp. Kor.	1,5	
Q50_kor	0,64	m3/s
Q50_kor	**2 300**	**m3/h**

Kryterium przepływu powietrza

Wyznaczenie przepływu przez drzwi

A_{VA}	2,64	m2
v	0,75	m/s
Q_{DO}	1,98	m3/s
Q_{DO}	**7 128**	**m3/h**
A_{VA}	**0,79**	**m2**

delta P	10	Pa
Kryterium 10Pa		
Ae(10)	2,64	m2
Q10_drzw	6,93	m3/s
przeplyw na drzwiach przy 10Pa Q10_drzw	**24 945**	**m3/h**
Qnieszcz_10	0,19	m3/s
przecieki przy 10Pa Qnieszcz_10	**686**	**m3/h**
Q10	7,12	m3/s
Suma Q10	**25 631**	**m3/h**
wsp_kor	1,15	
Q10_kor	**29 475**	**m3/h**
TOTAL	**29 475**	**m3/h**

obliczenia dla klatki wschodniej

Suma przeciekow	**0,07257**	**m2**	
Przecieki przez drzwi			
	ilosc	pow. nieszcz.	
Drzwi jednoskrzydl otw do przestrz o podw cisn	2	0,01	
Drzwi jednoskrzydl otw z przestrz o podw cisn	1	0,02	
Drzwi dwuskrzydl	0	0,03	
Ae_drzwi	**0,04**	**m2**	
Przecieki przez ściany wew			
szczelna		1,4E-05	
przeciętna		1,1E-04	
nieszczelna		3,5E-04	
A_ścian-wew	232	m2	
A_drzwi-wew	0	m2	
A_ścian netto-wew	232	m2	
Ae_ścian wew	**0,026**	**m2**	
Przecieki przez okna	ilosc	obwod	
rozwierane bez uszczeln	2	6,4	m
rozwierane z uszczeln	0	0	m
przesuwne	0	0	m
Ae_okien	**0,00320**	**m2**	
Przecieki przez stropy			
A_stropow	74,00	m2	
przeciętny	5,2E-05		
Ae_stropy	**0,004**	**m2**	
Przecieki przez ściany zew			
szczelna		7,0E-05	
przeciętna		2,1E-04	
nieszczelna		4,2E-04	
bardzo nieszczelna		1,3E-03	
A_ścian-zew	0	m2	
A_drzwi-zew	0	m2	
A_ścian netto-zew	0	m2	
Ae_ścian zew	**0,000**	**m2**	
Przecieki do szybu windy	Ilosc		Ae
Drzwi szybu windy w klatce schodowej	0		0
Drzwi szybu windy do innych pomieszczen	0		0
Otwor dla przewietrzania szybu windy	0	m2	
przecietna	0,00084		
Sciany szybu windy (z peknieciami w konstrukcji ale bez szczelin wokol okien i drzwi)	0	m2	0
Ogolna powierzchnia przeciekow do szybu windy	0,00000	m2	
Ogolna powierzchnia przeciekow z szybu windy	0,000	m2	
Powierzchnia nieszczelnosci dla szybu windy	**0,0000**	**m2**	

Klasa systemu	C

Predkosc powietrza na drzwiach otw [m/s]:	0,75
Drzwi zewnetrzne	zamkniete
Ilosc innych otwartych drzwi	0
Drzwi zewnetrzne dla kryterium nadcisnienia 10 Pa	otwarte
Ilosc innych drzwi otwartych dla kryterium nadcisnienia 10Pa	0

Kryterium różnicy ciśnienia
Wszystkie drzwi zamknięte

Qd	0,83*Ae*P^(1/R)	
Ae	0,0726	
P	50	
R	2	
Q50	0,43	m3/s
Q50	**1 533**	**m3/h**
wsp. Kor.	1,5	
Q50_kor	0,64	m3/s
Q50_kor	**2 300**	**m3/h**

Kryterium przepływu powietrza
Wyznaczenie przepływu przez drzwi

A_{VA}	2,64	m2
v	0,75	m/s
Q_{DO}	1,98	m3/s
Q_{DO}	**7 128**	**m3/h**
A_{VA}	**0,79**	**m2**

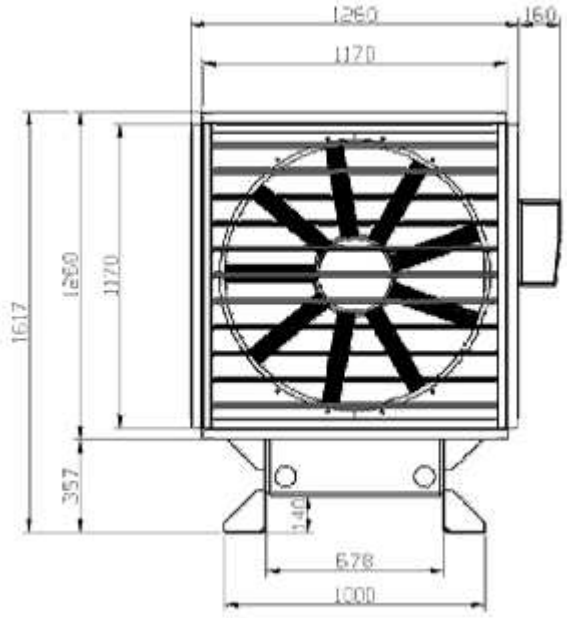
delta P	10	Pa
Kryterium 10Pa		
Ae(10)	2,64	m2
Q10_drzw	6,93	m3/s
przeplyw na drzwiach przy 10Pa Q10_drzw	**24 945**	**m3/h**
Qnieszcz_10	0,19	m3/s
przecieki przy 10Pa Qnieszcz_10	**686**	**m3/h**
Q10	7,12	m3/s
Suma Q10	**25 631**	**m3/h**
wsp_kor	1,15	
Q10_kor	**29 475**	**m3/h**
TOTAL	**29 475**	**m3/h**

Dobór urządzeń

Dla obu klatek schodowych analizowano i do obliczeń przyjęto urządzenie SMPA 100. MOżna zastosować rozwiązanie równoważne o nie gorszych parametrach technicznych. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

	Max wydatek	Spręż dyspozycyjny	Napięcie zasilania	Moc	Masa	Moc akustyczna*
SMPA 100	45 000	300	3x400	9	390	100

Wykonanie zewnętrzne z przepustnica wielopłaszczyznową po stronie ssawnej wentylatora.



Założono pracę urządzeni aa poziomie 60% - 70% wydajności. Pozwoli to na utrzymanie poziomu hałasu na poziomie 70 dB umożliwiając normalne działanie DSO.

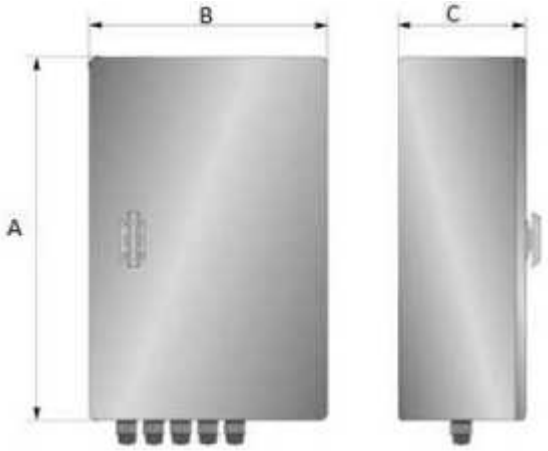
Urządzenia sterujące

Szafa zasilająco sterująca

Do szafy zasilająco sterującej schodzą się trasy kablowe wszystkich elementów systemu. Lokalizacja szafy powinna chronić ją od wpływu warunków atmosferycznych w szczególności niskich temperatur. Należy doprowadzić do niej zasilanie gwarantowane 3x400V oraz sygnał z

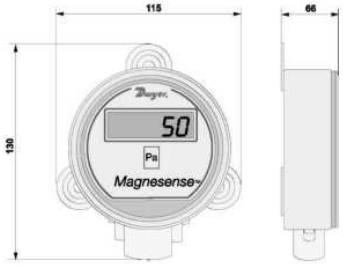
systemu SAP. Należy pamiętać o konieczności zapewnienia zasilania rezerwowego na wypadek awarii zasilania podstawowego w myśl normy PN-EN 12101-6.

	A	B	C
	[mm]	[mm]	[mm]
SMPA 100	700	700	300



Przetwornik różnicy ciśnienia

Przetwornik różnicy ciśnienia mierzy w sposób ciągły różnicę ciśnienia między przestrzenią chronioną (np. klatką schodową) a przestrzenią odniesienia (np. korytarzem ewakuacyjnym). Przetwornik posiada dwa króćce przyłączeniowe do których należy podłączyć rurki impulsowe zbierające sygnał ciśnienia (w przypadku lokalizacji przetwornika w obrębie przestrzeni chronionej nadciśnieniem, jeden z króćców należy pozostawić wolny). Podczas instalacji przetwornika szczególną uwagę należy zwrócić na prowadzenie rurki impulsowej w taki sposób aby nie uległa załamaniu oraz na lokalizację punktu pomiaru ciśnienia odniesienia uniemożliwiającego jego błędny odczyt.



Panel sterownia

Panel sterownia służy do zdalnej kontroli systemu oraz ręcznego uruchomienia bądź wyłączenia instalacji przez prowadzącego akcję gaśniczą. Wyposażony jest w kontrolki

stanu gotowości, pracy oraz awarii urządzenia.

Wytyczne dla branży elektrycznej

Zasilanie wentylatora systemu różnicowania ciśnień z przed wyłącznika pożarowego przewodem o dziewięćdziesięciominutowej odporności ogniowej.

Dla zapewnienia pracy systemu nadciśnieniowego na klatce schodowej wymagane jest zapewnienia zasilania trzema środkami:

W przypadku utraty zasilania podstawowego przejście na zasilanie rezerwowe musi następować automatycznie. Również powrót do stanu normalnego musi następować automatycznie. Pozycja gotowości i pozycja bezpieczeństwa będzie wskazywana na pulpicie sterowniczym.

Montaż instalacji

Montaż wykonywać zgodnie z DTR producenta, obowiązującymi w kraju normami i przepisami.

Montaż urządzenia wraz z systemem sterowania należy powierzyć osobom znającym wymagania normy PN-EN 12101-6 oraz dostarczającym urządzenia dopuszczone do używania w projektowanym przeznaczeniu.

Zaprojektowany system różnicowania ciśnienia na klatce schodowej musi zostać wytestowany próbą dymową i dopiero po sprawdzeniu jego skuteczności może zostać dopuszczony do użytkowania. Sprawdzeniu należy poddać skuteczność ochrony klatki schodowej prze zadymieniem, prędkość przepływu powietrza przez otwarte drzwi na piętro objęte pożarem, siłę otwierająca drzwi, która nie może przekraczać 100 N. Przy doborze samozamykacza drzwi należy uwzględnić istnienie systemu różnicowania ciśnień.

Urządzenie różnicowania systemu będzie sterowane przez bezpotencjałowy sygnał z systemu alarmu pożaru oraz system alarmu pożaru będzie monitorował start i awarię systemu.

Nadmiar powietrza dostający się z klatki schodowej na kondygnację przy otwartych drzwiach będzie usuwany przez żaluzję nad drzwiami na końcach korytarzy.

Zestawienie materiałów

nazwa	jm	ilość
Wentylator napowietrzający o wydajności min. 40 000 m^3/h wraz z systemem sterowania zapewniającym właściwe ciśnienie i czas reakcji krótszy niż 3s; Do analizy przyjęto SMPA-100 o wydajności 45 000 m^3/h. Można zastosować rozwiązanie równoważne o nie gorszych parametrach technicznych.	szt.	2
Moduł zasilnia SMPZ-2 z osprzętem i przewodami do wentylatora (zgodnie z DTR) lub równoważne	kpl.	2
Panel kontrolny SMPZ-3 lub równoważne	szt.	2
Przetwornik ciśnienia SMIZ-4 wraz z rurka impulsową 10 m lub równoważne		2
Siłowniki do żaluzji nad drzwiami na końcach korytarza	szt.	2
Centrala sterująca siłownikami okiennymi sterowana z SAP z akumulatorem podtrzymującym zasilanie.	szt.	2
Przewód E90 (3x1) (do siłowników)	m	120
Przewód E90 2x2x1 do przetwornika ciśnienia	m	20
Przewód E90 4x2x1 panela kontrolnego	m	20
Przewód E90 (3x2,5) (do zasilania centrali sterującej siłownikami okiennymi). Przekrój przewodu zasilającego należy sprawdzić ze względu na prąd i spadek napięcia	m	250
Przewód E90 (5x2,5 dla długości do 60m) (do zasilania wentylatora napowietrzającego). Przekrój przewodu zasilającego wentylator należy sprawdzić ze względu na prąd i spadek napięcia.	m	250

Można zastosować elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż przyjęte w projekcie. Zmiana elementów systemu na inny niż zaprojektowane wymaga ponownego wykonania obliczeń.
Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Dźwiękowy System Ostrzegawczy

Wymagania stawiane przed systemem DSO

Zgodnie z wymaganiami określonymi prawnie w stosownym rozporządzeniu oraz normie EN54 system DSO powinien spełniać poniższe kryteria:

- w przypadku wykrycia alarmu pożarowego i wysterowania przez system SSP, system DSO natychmiast staje się niezdolny do wykonywania funkcji nie związanych z ostrzeganiem o niebezpieczeństwie (takich jak przywoływanie, odtwarzanie muzyki lub uprzednio zapisanych informacji przesyłanych do głośników w obszarach wymagających transmisji alarmu),
- po włączeniu podstawowego lub awaryjnego (rezerwowego) źródła zasilania system jest zdolny do rozgłaszania w ciągu max 10s od zaistnienia stanu zagrożenia wynikającego ze zmiany położenia przekaźników strefowych SSP system jest zdolny do rozgłaszania sygnału ostrzegawczego, nadawanego przez operatora lub automatycznie, w ciągu max 3s,
- sygnały ostrzegawcze (modulowane) + przerwa od 4s do 10s poprzedzają pierwszy komunikat słowny. Sygnał ostrzegawczy oraz komunikat słowny powinny być nadawane kolejno bez przerwy, aż do zmiany zgodnej z procedurą ewakuacji, lub ręcznego wyciszenia. W przypadku pomieszczeń z długim czasem pogłosu, czas między powtarzanymi sekwencjami może zostać wydłużony do 30s, a sygnały ostrzegawcze powinny być rozgłaszane, wówczas gdy okresy ciszy powodowane innymi przyczynami przekraczają 10s,
- system jest zdolny do nadawania sygnałów ostrzegawczych i komunikatów słownych do jednego lub kilku obszarów jednocześnie, zgodnie z przyjętym sposobem alarmowania,
- uszkodzenie pojedynczego wzmacniacza lub linii głośnikowej nie powoduje całkowitej utraty obszaru pokrycia dźwiękiem,
- uszkodzenie pojedynczego wzmacniacza w systemie spowoduje automatyczne załączenie wzmacniacza rezerwowego,
- operator systemu jest w stanie stwierdzić na podstawie wskazań DSO prawidłowość działania lub nie działania systemu,
- przerwa w którejkolwiek linii strefowej spowoduje wyemitowanie sygnału alarmu o uszkodzeniu,

- uszkodzenia występujące w DSO są przekazywane do SSP za pośrednictwem nadzorowanego przez CSP połączenia. Przerwa w obwodzie łączącym przekaźnik alarmu o uszkodzeniu DSO z CSP powinna być wykrywana przez CSP.
- System posiada mechanizm bezpiecznego obejścia BY-PASS/CPU-OFF – umożliwiający przeprowadzenie ewakuacji budynku z poziomu wybranego mikrofonu strażaka w przypadku uszkodzenia kontrolera – z pominięciem tego ostatniego.

Organizacja ewakuacji wspomaganej przez system DSO

Dźwiękowy System Ostrzegawczy ma pełnić rolę systemu ostrzegania, radiowęzła odpowiedzialnego za odtwarzanie muzyki w tle (BGM) oraz umożliwić rozgłaszanie słownych komunikatów porządkowych lub informacyjnych. Najważniejszą funkcją dźwiękowego systemu ostrzegawczego jest umożliwienie rozgłaszania sygnałów ostrzegawczych i komunikatów głosowych dla potrzeb bezpieczeństwa osób przebywających w budynku. W tym celu system DSO należy zintegrować z Systemem Alarmowania o Pożarze (SAP). Wykrycie zagrożenia przez centralę SAP skutkować będzie aktywacją alarmu II stopnia.

Wraz z rozpoczęciem tego stanu centrala SAP wysteruje DSO w sposób zapewniający emisję komunikatu automatycznego o ewakuacji mobilizujący do natychmiastowego opuszczenia budynku. Szczegółowy scenariusz ewakuacji wraz z matrycą sterowań dla systemów DSO i SAP powinien zostać opracowany w oparciu o aktualną Instrukcją Bezpieczeństwa Pożarowego dla danego budynku.

Ze względu na specyfikę i budowę obiektu należy przygotować stosowne komunikaty w 3 językach: polskim, angielskim oraz niemieckim. Z tego względu system umożliwi przechowywanie w swojej pamięci wbudowanej przynamniej 16 komunikatów. Treść komunikatów uzgodnić należy z Zamawiającym.

System dawać będzie również możliwość swobodnego ‘ręcznego’ sterowania ewakuacją. W tym celu wyposażony on będzie w pojedynczy wyniesiony mikrofon strażaka zlokalizowany w pomieszczeniu Centrum 1.60.

Mikrofon strażaka:

- Będzie dawał możliwość wglądu w rodzaj komunikatu (automatycznego lub słownego) nadawanego przez system do poszczególnych stref, a także umożliwi zatrzymanie alarmowania automatycznego przez pracownika PSP kierującego akcją pożarową.
- Umożliwi manualne dokonanie wyboru stref zgodnie wiedzą o rzeczywistym stanie zagrożenia ludzi w budynku i nadanie dowolnego komunikatu do tych stref (komunikatów automatycznych: ewakuacyjnego lub ostrzegawczego, albo komunikatu słownego).

Mikrofon strażaka powinien sygnalizować jakąkolwiek usterkę systemu DSO, jeśli taka wystąpi, lecz nie później niż 100 sekund po jej wykryciu przez system.
Dodatkowo system wyposażony będzie w mikrofon strefowy do roli komercyjnych. Pulpit mikrofonu strefowego umożliwi nadawanie komunikatów ogólnych do wydzielonych stref nagłośnienia oraz kierowanie do tychże stref komunikatów ogólnych zapisanych w pamięci systemu. Pulpit ten będzie opatrzony poziomem priorytetu niższym niż mikrofon strażaka.
Liczba pulpitów mikrofonowych może być rozbudowana w późniejszym czasie. System powinien udostępniać możliwość obsługi przynajmniej 8 pulpitów.
System DSO przez cały czas pracy (w stanie dozoru, jak i alarmowania) kontrolować będzie wszystkie obwody wewnętrzne, w tym: elementy wykonawcze zlokalizowane w centrali SAP odpowiedzialne za wywołanie odpowiednich komunikatów w strefach pożarowych (przekaźniki sterujące), źródła automatycznych komunikatów alarmowych, magistrale komunikacyjne, przedwzmacniacze i wzmacniacze wraz ze wzmacniaczami rezerwowymi, a także linie głośnikowe dołączone do systemu. Nadzór obejmie również system zasilania podstawowego i rezerwowego.
Każda usterka powinna być sygnalizowana w ciągu maks. 100 sekund od wykrycia nieprawidłowości, w sposób widoczny określony w normie EN 54-16. Fakt wystąpienia awarii powinien być odnotowany w pamięci zdarzeń systemu, do której dostęp będzie posiadał wyłącznie wykwalifikowany personel.
Przynajmniej zbiorcza informacja o awarii (awaria ogólna) powinna być przekazana do centrali SAP. Połączenie to nadzoruje centrala SAP.

Strefy nagłośnienia

Obiekt został podzielony tak, że każda funkcjonalnie wydzielona przestrzeń stanowi oddzielną strefę nagłośnieniową. Na każdą z tych stref przewidziano redundancję linii głośnikowych (zdwojenie okablowania A+B), co zapewnia zachowanie ciągłości rozgłaszania w razie awarii pojedynczej linii głośnikowej w strefie. Wydzielenie stref odbywa się na zasadzie logicznego przypisania linii głośnikowych do zdefiniowanych stref ogniowych.
Obszar pokrycia dźwiękiem będzie obejmował wszystkie pomieszczenia (poza obszarami wyłączonymi z alarmowania). Do obszarów wyłączonych z alarmowania zalicza się:
- niewielkie pomieszczenia gospodarczo-techniczne, w których przewiduje się sporadyczne przebywanie ludzi w krótkim czasie (np.: szachty instalacyjne, szachty wind, małe magazyny. itp.)

- niewielkie pomieszczenia przejściowe, w których czas przebywania ludzi jest ograniczony do czasu potrzebnego na przejście pomiędzy pomieszczeniami objętymi DSO (np. przedsionki, małe korytarzyki, itp.)
- pomieszczenia gdzie nie przewiduje się obecności ludzi.

Zakłada się, iż system DSO pełnić będzie rolę systemu nagłośnienia informacyjnego z priorytetem nagłośnienia alarmowego. Umożliwiać on będzie emisję przynajmniej 4 sygnałów audio w tym samym czasie, przy czym nadawanie komunikatów głosowych przez operatorów pulpitów mikrofonowych do wybranych stref nie będzie skutkowało przerwaniem emisji podkładu muzycznego BGM w strefach pozostałych. Dodatkowo będzie istniała możliwość wykorzystania wejść lokalnych zastosowanych wzmacniaczy mocy do podłączenia niezależnych źródeł dźwięku obsługujących poszczególne strefy.

Wymagane parametry dźwięku

Zgodnie z wymogami dotyczącymi bezpieczeństwa system DSO powinien zapewnić uzyskanie odpowiednio wysokiej zrozumiałości mowy, która określona jest poprzez wartość współczynnika zrozumiałości mowy STIPA. Wartość średnia tego współczynnika pomniejszona o jego odchylenie standardowe w każdej nagłaśnianej powierzchni powinna przekraczać 0,5. Dodatkowo zapewniony zostanie odpowiedni odstęp sygnału użytecznego (tj. dźwięku bezpośredniego) od tła otoczenia (hałasu). Aby zapewnić możliwość uzyskania odpowiedniej zrozumiałości mowy odstęp ten powinien wynosić minimum 6 dB.

Dla określenia właściwego poziomu roboczego SPL dla głośników poziom hałasu otoczenia panującego w strefach do nagłośnienia przyjęto :

Pomieszczenia biurowe, klatki schodowe – 65dB(A)

Hole, korytarze, kuchnia – 72 dB(A)

Strefy otwarte parteru – 74 dB(A)

Pomieszczenia maszyn – 75 dB(A)

Pasmo użyteczne zastosowanych zestawów głośnikowych dostosowane będzie do roli pomieszczeń, w których zostaną one zainstalowane.

Linie głośnikowe

Linie głośnikowe wykonane będą w technice wysokonapięciowej 100V z przeplotem (A+B). Zrealizowane one będą okablowaniem spełniającym wymóg PH90 od głośnika do głośnik. Średnica przewodu dobrana będzie z uwzględnieniem mocy zestawów głośnikowych obsługiwanych na poszczególnych liniach oraz spadku napięcia na tychże liniach. Odcinki wewnętrzne linii głośnikowych poprowadzone będą w przestrzeni przysufitowej w korytach kablowych, na odpowiednich uchwytach zapewniających cechę PH90.

System DSO będzie realizował ciągły monitoring obsługiwanych linii głośnikowych (system wykryje ewentualne zwarcie, rozwarcie, i/lub doziemienie linii głośnikowej). Pomiar sprawności linii prowadzony będzie z wykorzystaniem metody impedancyjnej. System powinien umożliwić obsługę przynajmniej 60 linii głośnikowych.

W skład systemu DSO wchodzić będzie szereg zestawów głośnikowych dobranych pod kątem zapewnienia odpowiedniego pokrycia nagłaśnianych obszarów dźwiękiem oraz uzyskania wymaganej zrozumiałości reprodukowanej przez system mowy. Do nagłośnienia obiektu dobrane zostały 3 rodzaje zestawów głośnikowych:

Głośniki sufitowe 6W przeznaczone do nagłośnienia pomieszczeń ogólnych posiadających sufit podwieszany. Głośniki te będą się cechowały pasmem przenoszenia nie węższym niż od 100Hz do 16kHz oraz efektywnością rzędu 90 dB SPL (@1W/1m).

Przykładowa specyfikacja techniczna głośnika sufitowego zamieszczona jest w poniższej tabeli:

Rodzaj	Pożarowy głośnik sufitowy oznaczony w projekcie symbolem PC-1867FC L10A/03
Moc znamionowa	6W
Moc przepinana	100V: 6W (1,7 kOhm), 3W (3,3 kOhm), 1,5W (6,7 kOhm), 0,8W (13 kOhm)
Efektywność (1W/1m)	90 dB
Pasmo przenoszenia	100Hz – 16kHz
Typ głośnika	Typ A; głośnik do zastosowań wewnętrznych
Przetwornik	Pojedynczy głośnik stożkowy średnicy 12 centymetrów (5’’)
Przewód	Drut: AWG 20-14; linka: AWG 18-9
Konektor	Para kostek ceramicznych z bezpiecznikiem termicznym
Wykonanie	Obudowa: aluminium pokryte białą farbą (RAL 9010 lub odpowiednik) Maskownica: aluminium pokryte białą farbą (RAL 9010 lub odpowiednik) Uchwyt kopuły: chromowana płytka stalowa Kopuła przeciwogniowa: Płyta stalowa pokryta czarną farbą
Wymiary	Φ180 x 11 + 110 (Gł) mm
Waga	1,4 kg

Głośniki naścienne typu 1 dedykowane do nagłośnienia klatek schodowych, pomieszczeń technicznych oraz magazynów. Głośniki te cechować się będą efektywnością przynajmniej 89 dB SPL (@1W/1m) oraz mocą znamionową rzędu 6 Wat. Pasmo przenoszenia zestawów będzie niewęższe niż od 150Hz do 20kHz.

Przykładowa specyfikacja techniczna głośnika naściennego typu 1 zamieszczona jest w poniższej tabeli:

Rodzaj	Pożarowy głośnik naścienny typ 1 oznaczony na rysunku symbolem BS-680FC L12B/01
Moc znamionowa	6W
Moc przepinana	100V: 6W (1,7 kOhm), 3W (3,3 kOhm), 1,5W (6,7 kOhm), 0,8W (13 kOhm)
Efektywność (1W/1m)	89 dB
Pasmo przenoszenia	150Hz – 20kHz
Kąt promieniowania(-6dB)	500Hz: 180° (w obu płaszczyznach), 1kHz: 140° (w obu płaszczyznach), 2kHz: 120°x110° (H x V), 4kHz: 100°x80° (H x V)
Typ głośnika	Typ A; głośnik do zastosowań wewnętrznych
Przetwornik	Głośnik dwustożkowy średnicy 16cm (6’’)
Przewód	AWG 18-9
Konektor	Para kostek ceramicznych z bezpiecznikiem termicznym
Wykonanie	Obudowa: płyta stalowa pokryta białą farbą (RAL 9010 lub odpowiednik) Maskownica: powlekana powierzchniowo płyta stalowa pokryta białą farbą (RAL 9010 lub odpowiednik)
Wymiary	310 (Sz) x 190 (Wys) x 87,2 (Gł) mm
Waga	2,6 kg

Głośniki naścienne typu 2 dedykowane do nagłośnienia hollu obejmującego Strefę Ogólnodostępną, Strefę Przylotów, Strefę Odlotów oraz Tarasy Widokowe. Głośniki te będą miały dwudrożną konstrukcję typu Bass-Reflex zapewniającą wysoką jakość dźwięku. Cechować się będą pasmem przenoszenia przynajmniej od 80 Hz do 20 kHz, mocą znamionową rzędu 30W oraz efektywnością niemniejszą niż 90 dB SPL.

Przykładowa specyfikacja techniczna głośnika naściennego typu 2 zamieszczona jest w poniższej tabeli:

Rodzaj	Pożarowy głośnik naścienny typu 2 oznaczony na rysunku symbolem F-1300BTWP EB-Q L03A/04
Moc znamionowa	30 W
Moc przepinana	100V: 30W (330 Ohm), 10 W (1 kOhm), 3W (3,3 kOhm), 1W (10 kOhm)
Efektywność (1W/1m)	90 dB
Pasmo przenoszenia	80 Hz - 20 kHz
Komponenty głośnikowe	13-centymetrowy głośnik stożkowy + tweeter kopułkowy średnicy 25 mm
Częstotliwość podziału	2 kHz
Kąt promieniowania	110° x 100°
Przewód	AWG 18-13
Rodzaj konektora	Para kostek ceramicznych z bezpiecznikiem termicznym
Wykonanie	Obudowa z tworzywa HIPS, stalowa maskownica pokryta ochronną warstwą antykorozyjną, uchwyt naścienny i łączący ze stali nierdzewnej, uchwyt głośnikowy z odlewanego aluminium, zestaw w kolorze czarnym
Typ głośnika	Typ A; głośnik do zastosowań wewnętrznych
Zakres temperatury pracy	Od -10° C do +50° C
Wymiary	162 × 250 × 161 mm
Waga	3,6 kg
Akcesoria	Uchwyt głośnikowy (1x), uchwyt naścienny (1x), uchwyt łączący (1x), zestaw śrub do montażu uchwytu (1x), pokrywka terminalu głośnikowego (1x), śruba do montażu pokrywki terminala (4x)

Architektura systemu

W poniższym paragrafie przytoczona jest przykładowa konfiguracja systemu DSO. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe –

powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności system, komplikować jego obsługi, ani też degradować jakość reprodukowanego dźwięku. Wszelkie zmiany należy udokumentować poprzez załączenie do propozycji zmiany projektu systemu opisu technologicznego stosowanych urządzeń oraz sposobu ich połączenia w całość systemu. Zamiana zestawów głośnikowych powinna być poparta przeprowadzeniem symulacji akustycznych, które wykażą utrzymanie parametrów dźwięku takich jak poziom dźwięku bezpośredniego oraz zrozumiałość mowy (opisana współczynnikiem zrozumiałości mowy) w wymaganych granicach.

Projektuje się instalację systemu DSO o budowie modułowej i scentralizowanej architekturze. Elementem centralnym systemu będzie menadżer, który pełnić będzie jednocześnie rolę interfejsu wejściowego audio – pozwali na podłączenie wyniesionych pulpitów mikrofonowych oraz dodatkowych źródeł dźwięku w postaci np. odtwarzaczy CD, których rolą będzie emisja muzyki w wybranych strefach nagłośnienia. Menadżer systemu przechowywać będzie w swojej pamięci komunikaty (nie mniej niż 16), które mogą być wyzwalane w sposób automatyczny lub też ręczny. Menadżer będzie również prowadzić dziennik pracy systemu (dziennik przechowuje nie mnie niż 2000 zdarzeń).

Menadżer systemu DSO dopuszczać będzie zastosowanie dnie mniej niż 8 wyniesionych pulpitów mikrofonowych – komercyjnych i/lub strażaka w dowolnej kombinacji. Pulpity wyposażone w programowalne przyciski funkcyjne (z możliwością rozbudowy liczby przycisków przez zastosowanie dedykowanych rozszerzeń), które umożliwią:

- wyzwalanie komunikatu o ewakuacji (ręcznie),
- wyzwalanie komunikatu ostrzegawczego (ręcznie) ,
- kasowania stanu alarmu,
- wybór stref rozgłaszania.

Na ostatnim rozszerzeniu przycisków możliwe będzie wykorzystanie przycisków w celu sygnalizacji stanu awarii (w wykorzystaniem LED dostępnych przy przyciskach), dzięki czemu pulpit stanie się również tablicą kontrolną dla całego systemu, odczytującą stany jego stany awaryjne. System stale monitorować ma sprawność mikrofonu strażaka. Przyjęto monitoring metodą akustyczną, co pozwoli wykryć również awarię membrany mikrofonu niezwiązaną z zachowaniem ciągłości cewki.

Wszystkie pulpity mikrofonowe opatrzone będą priorytetami, przy czym mikrofony strażaka mają zawsze przypisany najwyższy priorytet, co oznacza, iż w przypadku słownego rozgłaszania o zagrożeniu przez mikrofon strażaka automatycznie zostaje wyciszony komunikat automatyczny. Bezpośrednio pod menadżer systemu podlegają jednostki zarządzające odpowiedzialne za matrycowanie sygnałów audio pomiędzy poszczególnymi wzmacniaczami mocy oraz kontrolę linii głośnikowych. Linie głośnikowe w systemie zasilane będą przy pomocy dedykowanych wzmacniaczy mocy dobranych spośród modeli: 1x 420W, 1x 240W, 2x 120W oraz 4x 60W w sposób gwarantujący wysterowanie zasilanych zestawów głośnikowych z odpowiednią mocą. Przewiduje się zastosowanie rezerwowych wzmacniaczy mocy tego samego rodzaju, które załączane będą automatycznie w momencie wykrycia awarii jednego ze wzmacniaczy podstawowych. System pozwoli na przyłączenie 1 wzmacniacza rezerwowego na 10 wzmacniaczy podstawowych.

Zaprojektowano własne zasilanie rezerwowe oparte na dedykowanych modułach zasilaczy i urządzeniach zarządzających, pełniących jednocześnie rolę ładowarek akumulatorów (stanowiących awaryjne zasilanie systemu). Ładowarki dostarczać będą napięcie stałe do wszystkich urządzeń wchodzących w skład systemu DSO oraz sprawować monitoring tego zasilania. W zaniku zasilania podstawowego, spowodowanego przerwą w zasilaniu sieciowym, jednostka zarządzająca systemem zasilania automatycznie przełączy urządzenia systemu na zasilanie rezerwowe z baterii akumulatorów. Jednostka w trakcie ładowania akumulatorów będzie mierzy ich temperaturę aby odpowiednio kompensować napięcie ładowania.

W skład systemu DSO obiektu wchodzić będą:

- 2 szafy Rack 19” 44U,
- wyniesiony mikron strażaka RM-200XF wraz z modułami rozszerzeń,
- wyniesionych mikrofonów strefowych RM-200X,
- głośniki pożarowe wraz z okablowaniem oraz inne urządzenia wymienione w poniższej tabeli.

Elementy centralne systemu ulokowane zostaną w Pomieszczeniu Technicznym Pom.1.95. Zarówno mikrofon strażaka jak i ogólny pulpit wywoławczy zainstalowane zostaną w Centrum Nadzoru Pom.1.60.

Zestawienie materiałów

Symbol	Opis	Ilość
VX-2000	Rama systemowa Dźwiękowego Systemu Ostrzegawczego VX-2000 lub rozwiązanie równoważne	1
VX-200XR	Moduł wejścia mikrofonu wyniesionego lub rozwiązanie równoważne	3
U-03R	Moduł stereofonicznego wejścia liniowego systemu VX-2000; na konektorach RCA, niezbalansowane, monofonizowane, lub rozwiązanie równoważne	1
EV-200M	Płytka zapowiedzi głosowych do odtwarzania komunikatów głosowych lub rozwiązanie równoważne	2
RM-200XF	Pulpit mikrofonu strażaka lub rozwiązanie równoważne	1
RM-200XS	Pulpit mikrofonu wywoławczego lub rozwiązanie równoważne	2
RM-320F	Rozszerzenie do mikr. strażaka; 20 przycisków lub rozwiązanie równoważne	1
RM-210	Rozszerzenie do pulpitu wywoławczego; 10 przycisków lub rozwiązanie równoważne	2
VX-2000SF	Rama monitorująca Dźwiękowego Systemu Ostrzegawczego VX-2000 lub rozwiązanie równoważne	2
VX-200SZ	Moduł kontroli impedancji linii głośnikowej lub rozwiązanie równoważne	6
VX-200SZ-2	Dwukanałowy (A+B) moduł kontroli impedancji linii głośnikowej lub rozwiązanie równoważne	9
VX-200SI	Moduł sterowania systemu VX-2000; wyposażony w 16 wejść sterujących typu beznapięciowy styk zwarciowy, na konektorach RJ-45 lub rozwiązanie równoważne	2
VP-2064	Wzmacniacz systemowy DSO 4x60W; do stosowanie wymaga modułu wejściowego VP-200VX/VP-200VX-BGM; wymaga zasilania DC lub rozwiązanie równoważne	1
VP-2122	Wzmacniacz systemowy DSO 2x120W; do stosowanie wymaga modułu wejściowego VP-200VX/VP-200VX-BGM; wymaga zasilania DC lub rozwiązanie równoważne	1

Symbol	Opis	Ilość
VP-2241	Wzmacniacz systemowy DSO 1x240W; do stosowanie wymaga modułu wejściowego VP-200VX/VP-200VX-BGM; wymaga zasilania DC lub rozwiązanie równoważne	8
VP-2421	Wzmacniacz systemowy DSO 1x420W; do stosowania wymaga modułu wejściowego VP-200VX/VP-200VX-BGM; wymaga zasilania DC lub rozwiązanie równoważne	5
VP-200VX	Moduł wejściowy audio i sterowania do wzmacniaczy lub rozwiązanie równoważne	4
VP-200VX BGM	Moduł wejściowy audio i sterowania z wejściem lokalnym audio lub rozwiązanie równoważne	13
URD-1000	Odtwarzasz CD/SD/USB + TUNER lub rozwiązanie równoważne	1
WB-RM200	Uchwyt dla mikrofonu informacyjnego lub rozwiązanie równoważne	1
VX-2000PF	Rama do montażu zasilaczy systemowych typu VX-200PS lub rozwiązanie równoważne	3
VX-200PS	Zasilacz systemowy DSO 580W lub rozwiązanie równoważne	8
VX-2000DS	Dystrybutor zasilania do stosowania w systemach DSO lub rozwiązanie równoważne	3
CR-44	Szafa rack 44U lub rozwiązanie równoważne	2
RH 452	Obudowa mikrofonu strażaka 400x500x150 lub rozwiązanie równoważne	1
EPS 65-12 PL	akumulator 12 V 65 Ah lub rozwiązanie równoważne	4
EPL 85-12 PL	akumulator 12 V 85 Ah lub rozwiązanie równoważne	2
BS-680FC	Pożarowy głośnik naścienny 6W w solidnej metalowej obudowie efektywność 94 dB SPL; pasmo przenoszenia 150Hz - 20kHz lub rozwiązanie równoważne	26
PC-1867FC	Pożarowy głośnik sufitowy 6W efektywność 89 dB SPL; pasmo przenoszenia 100Hz - 16kHz lub rozwiązanie równoważne	199

Symbol	Opis	Ilość
F-1300BTWP EB-Q	Dwudrożny głośnik naścienny o szerokim kącie promieniowania efektywność 90 dB SPL, moc znamionowa 30W, pasmo przenoszenia 80Hz - 20kHz lub rozwiązanie równoważne	100
HDGs 2x1,5 PH90	Przewód ognioodporny ognioodporne HDGs 2x1,5 300/500 V lub rozwiązanie równoważne	7200 mbr.
HTKSHekw 4x2x1 PH90	Przewód ognioodporny HTKSHekw PH90 4x2x1 lub rozwiązanie równoważne	50 mbr.
HDGs 3x2,5	Przewód ognioodporny HDGszo 3x2,5 300/500 V lub rozwiązanie równoważne	100 mbr.
OBO 1015 - 12mm	Obejmy kablowe lub rozwiązanie równoważne	2400
FDN 6x65	Gwóźdź stalowy 6x65mm lub rozwiązanie równoważne	2460

Można zastosować elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż analizowane w projekcie. Zmiana elementów systemu na inny niż zaprojektowane wymaga ponownego wykonania obliczeń.
Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Okablowanie strukturalne

Okablowanie strukturalne będzie zbudowane w typologii hierarchicznej gwiazdy. Stanowiska robocze obsługiwane będą przez podsystemy okablowania poziomego. Podsystemy obejmują funkcjonalne wydzielanie sieci dla poszczególnych służb i zastosowań: sieć Straży Granicznej, sieć Służby Celnej, sieć na potrzeby urządzeń bezpieczeństwa i sieć administracyjna..

Okablowanie poziome będzie wykonane z użyciem czteroparowej ekranowej skrętki kat. 6A o gwarantowanej transmisji 500 MHz. Dwa oddzielne kable przewidziano dla każdego stanowiska roboczego (punktu) okablowania. Każdy z nich rozszyty będzie w modularnym gnieździe RJ45. Każde stanowisko robocze będzie wyposażone w dwa takie gniazda. Przyłącza do budynku nie są w zakresie projektu.

Architektura systemu

Okablowanie strukturalne zostało zaprojektowane na potrzeby:

1. administracji lotniskiem, obsługi aplikacji lotniskowych - oznaczone symbolem LOT
2. urządzeń służących do połączenia urządzeń bezpieczeństwa pasażerów - oznaczone symbolem SOL,
3. Straży Granicznej - oznaczone symbolem SG,
4. Służby Celnej - oznaczone symbolem SC,
5. monitoringu wizyjnego (CCTV).

Wszystkie te sieci są niezależne o odseparowane fizycznie od siebie. Istnieje możliwość przesyłania informacji między sieciami jedynie na poziomie przyłącza do budynku w szafie przyłączy. Dla każdej z sieci zaprojektowano oddzielną serwerownię wyposażoną w szafę LAn i szafę przewidzianą dla serwerów. W okablowaniu strukturalnym LOT zaprojektowano szafę FIS, a w okablowaniu SOL szafę CCTV i szafę dla systemów bezpieczeństwa pasażerów.

Serwerownię zaprojektowano jako jedno pomieszczenie wydzielone pożarowo do reszty budynku z podziałem na poszczególnych użytkowników z zastosowaniem ażurowych ścian działowych według projektu architektonicznego. W serwerowni zaprojektowano wentylację z redundancja urządzeń według projektu branży wentylacyjnej.

Ze względu na wielkość budynku i przekraczanie normowej długości przewodu od gniazda do punktu dystrybucyjnego, zaprojektowano dwa Lokalne Punkty Dystrybucyjne. Na rzutach oznaczono powierzchnie obsługiwane przez poszczególne punkty dystrybucyjne.

Wszystkie węzły okablowania zabezpieczone sa przez kontrolę dostępu i system sygnalizacji włamania. Serwerownie dodatkowo wyposażono w kamery monitorujące.

Wymagania dotyczące systemu i komponentów instalowanego okablowania strukturalnego

Wszystkie elementy pasywne projektowanej sieci muszą pochodzić od jednego producenta co umożliwi uzyskanie całościowej i spójnej gwarancji na cały system. Projektuje się rozwiązanie, które ma pochodzić od jednego producenta i być objęte jednolitą i spójną gwarancją systemową producenta na okres minimum 25 lat obejmującą wszystkie elementy pasywne toru transmisyjnego, jak również płyty czołowe gniazd abonenckich, wieszaki kablowe i szafy dystrybucyjne.

Wymaga się, aby 25-letnia gwarancja była standardowym elementem w ofercie producenta, nie może być oferowana „specjalnie dla tej inwestycji" przez wykonawcę, dostawcę, dystrybutora, a nawet przez producenta;

Wszystkie elementy okablowania (w szczególności: panele krosowe, gniazda, kabel, szafy, kable krosowe, płyty czołowe gniazd, prowadnice kablowe i inne) mają być oznaczone logo lub nazwą tego samego producenta i pochodzić z oferty rynkowej producenta. Wszystkie podsystemy, tj. system okablowania logicznego (i telefonicznego) muszą być opracowane (tj. zaprojektowane, wykonane i wdrożone do oferty rynkowej) przez producenta jako kompletne rozwiązania, celem uzyskania maksymalnych zapasów transmisyjnych (marginesów pracy). Niedopuszczalne jest stosowanie rozwiązań „składanych" od różnych dostawców komponentów (różne źródła dostaw kabli, modułów gniazd RJ45, paneli, kabli krosowych, itd). Producent oferowanego systemu okablowania strukturalnego musi spełniać najwyższe wymagania jakościowe potwierdzone następującymi programami i certyfikatami np: Six Sigma, ISO 9001, GHMT Premium Verification Program.

Wszystkie komponenty systemu okablowania mają być zgodne z wymaganiami obowiązujących norm wg.: ISO/IEC 11801:2011 wyd.2.2, EN-50173-1:2011, PN-EN 50173-1:2011, IEC 61156-5 wyd.2, ANSI/TIA/EIA 568-C.2. Producent systemu musi przedstawić odpowiednie certyfikaty niezależnego laboratorium, np. 3P,DELTA Electronics, GHMT, ETL SEMKO potwierdzające zgodność wszystkich elementów systemu z wymienionymi w tym punkcie normami.

W celu zagwarantowania Użytkownikowi końcowemu najwyższej jakości parametrów technicznych i użytkowych cała instalacja musi być nadzorowana w trakcie budowy oraz

zweryfikowana przez inżynierów ze strony producenta przed odbiorem technicznym.

Aby zainstalowana sieć przez cały okres trwania 25 letniej gwarancji zapewniała pełną wydajność - system Cat.6A / klasa EA musi przewyższać wymagania standardów okablowania strukturalnego w szczególności ISO 11801 ed.2.2 na kanał i łącze stałe o min. 3dB. Wydajność komponentów (złącze-wtyk) ma być potwierdzona certyfikatem Re-Embedded Testing wystawionym przez niezależne laboratorium badawcze. System ma się składać w pełni z ekranowanych elementów, to wymaganie dotyczy zarówno gniazd końcowych jak i paneli krosowych. Zgodnie z wymaganiami norm każdy 4-parowy kabel ma być w całości (wszystkie pary) trwale zakończony na 8-pozycyjnym złączu modularnym - tj. na ekranowanym module gniazda RJ45 skonstruowanym w oparciu o technologię IDC. Niedopuszczalne są żadne zmiany w zakończeniu par transmisyjnych kabla. Konstrukcja paneli krosowniczych ma zapewniać optymalne wyprowadzenie kabla bez zagięć i załamań, przy pomocy poziomych paneli porządkowych. W celu zagwarantowania najwyższej jakości połączenia, a przede wszystkim powtarzalnych parametrów, wszystkie złącza, zarówno w gniazdach końcowych, panelach oraz złączach RJ45 w kablach krosowych i przyłączeniowych muszą być zarabiane w oparciu o technologię IDC. Proces montażu modułów gniazd RJ45 ma gwarantować najwyższą powtarzalność. Maksymalny rozplot par transmisyjnych na modułach gniazd RJ45 montowanych zarówno w panelach, jak i w zestawach instalacyjnych naściennych nie może być większy niż 8 mm. Ze względu na wymaganą najwyższą długoterminową trwałość i niezawodność oraz parametry kontaktu należy stosować kable przyłączeniowe i krosowe wykonane i przetestowane przez producenta.

Okablowanie poziome

Zaprojektowano okablowanie miedziane kategorii $Kat.6_A$ (wg ISO) z wykorzystaniem kabla ekranowanego S/FTP. Kabel prowadzony w listwach kablowych oaz korytach kablowych. Kable miedziane należy zakończyć w punktach dystrybucyjnych z 10 m zapasem. Maksymalna długość kabla między panelem a gniazdem abonenckim nie może przekroczyć 90m. Lokalizacja gniazd jest uzgodniona z użytkownikiem. Moduły gniazd montowane na listwach instalacyjnych z wykorzystaniem komponentów (mocowań i ramek) systemowych producenta listew instalacyjnych. Lokalizacja gniazd zgodnie z rysunkiem.

Prowadzenie okablowania w budynku

Okablowanie należy prowadzić w korytach kablowych, kanałach podpodłogowych, rurach

instalacyjnych w ścianach i pod podłogą.

Na stropie kondygnacji +1 w przestrzeni technicznej zaprojektowano koryta kablowe o wymiarach 200x100 przeznaczone dla okablowania strukturalnego.

Pod podłogą podniesioną na kondygnacji +1 okablowanie prowadzić w korytach kablowych 200x40.

Koryta kablowe informacje:

Zastosowanie: Prowadzenie trasy kablowej.

Materiał: Stal cynkowana metodą Sendzimira PN-EN 10346:2011.

Możliwość łączenia koryt poprzez wsuwanie jednego w drugie i montaż bez łączników.

Do montażu należy użyć komplety śrubowe M6x12 lub M6x12.

Przy montażu koryt należy stosować oryginalne elementy mocujące i kształtki.

Pod posadzką hali okablowanie prowadzić w korytach podposadzkowych 175H38/3 trzytorowych lub rurach instalacyjnych karbowanych gładkich w środku DVK fi 50mm. Przy układaniu rur należy przestrzegać minimalnego promienia gięcia, który dla zaprojektowanych rur wynosi 25 średnic.

W budynku zaprojektowano kanał kablowy prowadzący wzdłuż budynku. W kanale przewody okablowania strukturalnego układać na korytach kablowych 200x100mm na dwóch poziomach. Trzeci poziom z korytem 200x40mm przeznaczony jest dla okablowania systemów teletechnicznych. Koryta dla kabli słaboprądowych zamontować do ściany koryta po jednej stronie kanału zostawiając drugą stroną na potrzeby okablowania elektrycznego.

W ścianach przewody prowadzić w rurach instalacyjnych karbowanych o średnicy 20 mm.

Przy lokalizacji gniazd w podłodze należy użyć puszek 2x4M (gdzie M oznacza moduł Mosaic 22,5mmx45mm) np. Baks UDH E2 510 lub puszek Baks UDH Q3 514. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Okablowanie pionowe

Zaprojektowano połączenia pomiędzy GPD i LPD: 8xS/FTP, 4OS1, 4OM3. Na schemacie pokazano wyposażenie szaf i sposób wykonania połączeń.

Okablowanie łączące punkty dystrybucyjne (sieć szkieletowa, okablowanie pionowe) jest

zaprojektowane kablem miedzianym S/FTP 8 x, światłowodowym kablem wielomodowym OM4 4 włókna i światłowodowym kablem jednomodowym OS1 4 włókna..

Sieć bezprzewodowa

W opracowaniu okablowania strukturalnego zawarto również gniazda abonenckie zaprojektowane dla sieci bezprzewodowej. Gniazda zlokalizowano tak jak na rzutach budynków. Gniazda dedykowane dla sieci WiFi należy montować na ścianie 20 cm od sufitu lub na suficie. Gniazda przyłączeniowe sieci bezprzewodowej zakończona na oddzielnych panelach rozdzielczych w szafach dystrybucyjnych. Zasilanie urządzeń (acces point) sieci WiFi zaprojektowano w standardzie PoE (power over ethernet) za pomocą kabla sygnałowego sieci okablowania strukturalnego.

Punkty dostępowe

Zaprojektowano punkty dostępowe access-point zgodne ze standardami 802.11a/b/g/n oraz zasilane poprzez kabel sygnałowy Ethernet zgodnie ze standardem IEEE 802.3af lub IEEE 802.3at.

Połączenia światłowodowe w kanalizacji teletechnicznej

Zaprojektowano połączenia światłowodowe do kamer zewnętrznych CCTV zlokalizowanych na słupach oświetleniowych. Na planie terenu pokazano kanalizację teletechniczną. Kabel światłowodowy należy układać w kanalizacji wtórnej w kanalizacji teletechnicznej. Kabel światłowodowy, po wprowadzeniu do budynku należy zakończyć na przełącznicy światłowodowej szafy przyłączeniowej z pozostawieniem zapasu co najmniej 10 m strony budynku. Na słupie oświetleniowym kabel zakończyć w skrzynce rozdzielczej. dedykowanej dla instalacji teletechnicznych gdzie zaprojektowano mediakonwenter. Do połączenia zaprojektowano kabel światłowodowy jednomodowy OS1.

Wymagania gwarancyjne okablowania strukturalnego

Całość rozwiązania ma być objęta jednolitą, spójną 25-letnią gwarancją systemową producenta, obejmującą całą część transmisyjną „miedzianą" wraz z kablami krosowymi i innymi elementami dodatkowymi. Gwarancja ma być udzielona przez producenta bezpośrednio klientowi końcowemu. Gwarancja systemowa ma obejmować:

- gwarancję produktową (Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź 25-letniej eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione)
- gwarancję parametrów łącza/kanału (Producent zagwarantuje, że łącze stałe bądź kanał transmisyjny zbudowany z jego komponentów przez okres 25 lat będzie charakteryzował się parametrami transmisyjnymi przewyższającymi wymogi stawiane przez normę ISO/IEC11801 2nd edition:2002 dla klasy EA)
- wieczystą gwarancję aplikacji (Producent zagwarantuje, że na jego systemie okablowania przez okres „życia" zainstalowanej sieci będą pracowały dowolne aplikacje (współczesne i stworzone w przyszłości), które zaprojektowane były (lub będą) dla systemów okablowania klasy E (w rozumieniu normy ISO/IEC 118012nd edition:2002).

  Wymagana gwarancja ma być bezpłatną usługą serwisowa oferowaną Użytkownikowi końcowemu (Inwestorowi) przez producenta okablowania. Ma obejmować swoim zakresem całość systemu okablowania od Głównego Punktu Dystrybucyjnego do gniazda Użytkownika, w tym również okablowanie szkieletowe i poziome, zarówno dla projektowanej części logicznej jak i telefonicznej. W celu uzyskania tego rodzaju gwarancji cały system musi być zainstalowany przez firmę instalacyjną posiadającą status Partnera (co najmniej 2 przeszkolonych pracowników z ważnymi certyfikatami instalatorskimi) uprawniający do udzielenia gwarancji producenta.

  Wniosek o udzielenie gwarancji składany przez firmę instalacyjną do producenta ma zawierać: listę zainstalowanych elementów systemu zakupionych w autoryzowanej sieci sprzedaży w Polsce, wyniki pomiarów dynamicznych kanału lub łącza stałego wszystkich torów transmisyjnych według norm ISO/IEC 11801:2002 wyd. drugie lub EN 50173-1:2007, rysunki i schematy wykonanej instalacji. W celu zabezpieczenia interesu Użytkownika końcowego by dowieść zdolności udzielenia gwarancji 25-letniej systemowej producenta systemu okablowania - Użytkownikowi końcowemu (lub Inwestorowi) wykonawca okablowania (firma instalacyjna) powinien przedstawić:
  - dokument (imienny) poświadczający ukończenie kursu certyfikacyjnego przez zatrudnionego pracownika - wydany bezterminowo przez producenta (a nie w imieniu producenta). Dopuszczane są certyfikaty wydane w języku innym niż polski;
  - wykonawca okablowania strukturalnego winien wykazać się udokumentowaną, kompleksową realizacją projektów z zakresu IT - Data i Voice tzn. dostawą sprzętu aktywnego z konfiguracją, wraz z budową infrastruktury pasywnej.

Administracja i dokumentacja

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, tak od strony gniazda, jak i od strony szafy montażowej. Te same oznaczenia należy umieścić w sposób trwały na gniazdach sygnałowych w punktach przyłączeniowych użytkowników oraz na panelach. Powykonawczo należy sporządzić dokumentację instalacji kablowej uwzględniając wszelkie, ewentualne zmiany w trasach kablowych i rzeczywiste rozmieszczenie punktów przyłączeniowych w pomieszczeniach. Do dokumentacji należy dołączyć raporty z pomiarów torów sygnałowych.

Odbiór i pomiary sieci

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest uzyskanie gwarancji systemowej producenta potwierdzającej weryfikację wszystkich zainstalowanych torów na zgodność parametrów z wymaganiami norm Klasy EA Kategorii 6A wg obowiązujących norm. W celu odbioru instalacji okablowania strukturalnego należy spełnić następujące warunki:

1) **<u>Wykonać komplet pomiarów (pomiary części miedzianej i światłowodowej)</u>**

a) Pomiary należy wykonać miernikiem dynamicznym (analizatorem), który posiada wgrane oprogramowanie umożliwiające pomiar parametrów według aktualnie obowiązujących standardów. Analizator pomiarów musi posiadać aktualny certyfikat potwierdzający dokładność jego wskazań.

b) Analizator okablowania wykorzystany do pomiarów sieci musi charakteryzować się minimum III poziomem dokładności wg IEC 61935-1/Ed.3 i umożliwiać pomiar systemów w wymaganym paśmie.

c) Pomiary torów miedzianych należy wykonać w konfiguracji pomiarowej kanału transmisyjnego lub łącza stałego. W przypadku pomiarów kanału transmisyjnego procedura wymaga, aby po wykonaniu pomiarów jednego kanału, pozostawić tam kable krosowe, które były używane do pomiaru, zaś do pomiaru nowego kanału transmisyjnego należy rozpakować nowy kpl. kabli krosowych.

d) Pomiar każdego toru transmisyjnego poziomego (miedzianego) powinien zawierać:

    - Specyfikację (normę) wg której jest wykonywany pomiar

- Mapa połączeń
- Impedancja
- Rezystancja pętli stałoprądowej
- Prędkość propagacji
- Opóźnienie propagacji
- Tłumienie

- Zmniejszenie przesłuchu zbliżnego
- Sumaryczne zmniejszenie przesłuchu zbliżnego
- Stratność odbiciowa
- Zmniejszenie przesłuchu zdalnego
- Zmniejszenie przesłuchu zdalnego w odniesieniu do długości linii transmisyjnej
- Sumaryczne zmniejszenie przesłuchu zdalnego w odniesieniu do długości linii transmisyjnej
- Współczynnik tłumienia w odniesieniu do zmniejszenia przesłuchu
- Sumaryczny współczynnik tłumienia w odniesieniu do zmniejszenia przesłuchu
- Podane wartości graniczne (limit)
- Podane zapasy (najgorszy przypadek)
- Informację o końcowym rezultacie pomiaru

a) Pomiar każdego toru transmisyjnego światłowodowego (wartość tłumienia) należy wykonać dwukierunkowo (A>B i B>A) dla dwóch okien transmisyjnych, tj. 1310nm i 1550nm dla jednomodu (SM) . Pomiar powinien zawierać:

- Specyfikację (normę) wg, której jest wykonywany pomiar
- Metodę referencji
- Tłumienie toru pomiarowego
- Podane wartości graniczne (limit)
- Podane zapasy (najgorszy przypadek)
- Informację o końcowym rezultacie pomiaru
- Pomiary części światłowodowej należy wykonać przy wykorzystaniu odpowiednich końcówek pomiarowych do w/w urządzeń pomiarowych. W przypadku wykorzystania końcówek pomiarowych do analizatorów okablowania wymienionych powyżej należy dokonać pomiaru przy ustawieniu miernika w konfiguracji OF-2000 dla SM.

1) Na raportach pomiarów powinna znaleźć się informacja opisująca wysokość marginesu pracy (inaczej zapasu lub marginesu bezpieczeństwa, tj. różnicy pomiędzy wymaganiem normy a pomiarem, zazwyczaj wyrażana w jednostkach odpowiednich dla każdej wielkości mierzonej) podanych przy najgorszych przypadkach. Parametry transmisyjne muszą być poddane analizie w całej wymaganej dziedzinie częstotliwości/tłumienia. Zapasy (margines bezpieczeństwa) musi być podany na raporcie pomiarowym dla każdego oddzielnego toru transmisyjnego miedzianego oraz toru światłowodowego.

2) <u>Zastosować się do procedur certyfikacji okablowania producenta</u>

Obowiązująca procedura certyfikacyjna wymaga spełnienia następujących warunków:

- Dostawy rozwiązań i elementów zatwierdzonych w projektach wykonawczych zgodnie z obowiązującą w Polsce oficjalną drogą dystrybucji
- Przedstawienia producentowi faktury zakupu towaru (listy produktów) nabytego u Autoryzowanego Dystrybutora w Polsce.
- Wykonania okablowania strukturalnego w całkowitej zgodności z obowiązującymi normami ISO/IEC 11801, EN 50173-1, EN 50174-1, EN 50174-2 dotyczącymi parametrów technicznych okablowania, jak również procedur instalacji i administracji.
- Potwierdzenia parametrów transmisyjnych zbudowanego okablowania na zgodność z obowiązującymi normami przez przedstawienie certyfikatów pomiarowych wszystkich torów transmisyjnych miedzianych.
- Wykonawca musi posiadać status Autoryzowanego Partnera producenta okablowania.
- W celu zagwarantowania Użytkownikom końcowym najwyższej jakości parametrów technicznych i użytkowych, cała instalacja jest weryfikowana przez inżynierów ze strony producenta.

3) Wykonać dokumentację powykonawczą i przekazać ją Użytkownikowi.

Dokumentacja powykonawcza ma zawierać:

- Raporty z pomiarów dynamicznych okablowania,
- Rzeczywiste trasy prowadzenia kabli transmisyjnych poziomych
- Oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych
- Lokalizację przebić przez ściany i podłogi.
- Raporty pomiarowe wszystkich torów transmisyjnych należy zawrzeć w dokumentacji powykonawczej i przekazać inwestorowi przy odbiorze inwestycji. Drugą kopię pomiarów (dokumentacji powykonawczej) należy przekazać producentowi okablowania w celu udzielenia inwestorowi (Użytkownikowi końcowemu) bezpłatnej gwarancji.

4) Uwagi końcowe

Trasy prowadzenia przewodów transmisyjnych okablowania poziomego zostały skoordynowane z istniejącymi i wykonywanymi instalacjami w budynku m.in. dedykowaną oraz ogólną instalacją elektryczną, instalacją centralnego ogrzewania, wody, gazu, itp. Jeżeli w trakcie realizacji nastąpią zmiany tras prowadzenia instalacji okablowania (lub innych wymienionych wyżej) - należy ustalić właściwe rozprowadzenie z Projektantem działającym w porozumieniu z Użytkownikiem końcowym.

Wszystkie korytka metalowe, drabinki kablowe, szafy kablowe 19" wraz z osprzętem, łączówki telefoniczne wyposażone w grzebienie uziemiające oraz urządzenia aktywne sieci teleinformatycznej muszą być uziemione by zapobiec powstawaniu zakłóceń. Dedykowaną dla okablowania instalację elektryczną należy wykonać zgodnie z obowiązującymi normami i przepisami. W przypadku jakichkolwiek rozbieżności w dokumentacji, należy pisemnie zgłosić problem projektantowi, który zobowiązany jest do rozstrzygnięcia.

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

Różnice pomiędzy wymienionymi normami w projekcie a proponowanymi normami zamiennymi muszą być w pełni opisane przez Wykonawcę i przedłożone do zatwierdzenia przez Biuro Projektów na 30 dni przed terminem, w którym Wykonawca życzy sobie otrzymać zgodę. W przypadku, kiedy ustali się, że proponowane odchylenia nie zapewniają zasadniczo równorzędnego działania, Wykonawca zastosuje się do wymienionych w dokumentacji projektowej.

Kanalizacja pierwotna

Zaprojektowano kanalizację teletechniczną na potrzeby doprowadzenia kabli światłowodowych do kamer zewnętrznych na przyszłe potrzeby obsługi lotniska.

Przy budynku zaprojektowano studnię SKMP-3. Od studni zaprojektowano kanalizacje wprowadzeniową 9 rur fi100 prowadzonych w jednej warstwie pod posadzką klatki schodowej do szachtu teletechnicznego prowadzącego na kondygnację +1 do pomieszczenia technicznego gdzie znajduje się szafa przyłączeniowa. Rury należy ułożyć z zachowaniem minimalnego , dopuszczonego promienia gięcia i zaopatrzyć w piloty umożliwiające zaciąganie kabli i kanalizacji wtórnej. Studnia SKMP-3 może być wykorzystana do przyjęcia innych, zaprojektowanych dla potrzeb obsługi lotniska, ciągów kanalizacji teletechnicznej. Od studni SKMP-3 zaprojektowano kanalizację czterorurową do studni SKR-2 zlokalizowanej na rogu budynku. Studnia ta może być wykorzystana do przyjęcia innych, zaprojektowanych dla potrzeb obsługi lotniska, ciągów kanalizacji teletechnicznej. Dalej zaprojektowano dwururową kanalizację ze studniami SK2 w miejscach przyłączenia urządzeń CCTV i studniami SKR-2 w miejscach potencjalnych skrzyżowań z ciągami innych ciągów kanalizacji teletechnicznych.

Głębokość ułożenia rur kanalizacji kablowej powinna nie mniejsza niż 0,6 m, licząc od poziomu nawierzchni do górnej powierzchni kanalizacji. W sytuacjach uzasadnionych trudnościami technicznymi dopuszcza się zmniejszenie głębokości ułożenia kanalizacji pod warunkiem jej odpowiedniego zabezpieczenia, np. ławą betonową lub wykonania kanalizacji z grubościennych rur z tworzywa sztucznego bądź rur stalowych; grubość warstwy przykrycia

kanalizacji powinna wynosić co najmniej 0,2 m. W pokrywach studzien należy umieszczać wietrzniki w każdej studni, z której jest wykonane wprowadzenie kabli do budynku. Skrzyżowania telekomunikacyjnej kanalizacji pierwotnej z gazociągami powinno być wykonane zgodnie z Polskimi Normami. W razie skrzyżowania kanalizacji kablowej z rurociągami i urządzeniami do przesyłania płynów najmniejsze dopuszczalne odległości pionowe między nimi powinny wynosić :

a) od wodociągu magistralnego 0,25 m

b) od wodociągu rozdzielczego 0,15 m

c) obudowy sieci cieplnej, w tym sieci preizolowanej 0,50 m

d) ropociągu lub rurociągu dla produktów naftowych 0,80 m

e) od przewodów kanalizacji ściekowej 0,30 m

Skrzyżowania powinny być wykonane prostopadle z dopuszczalnym odchyleniem o 10° dla kanalizacji ściekowej i 35° dla pozostałych urządzeń. Kanalizacja kablowa powinna znajdować się nad tymi urządzeniami. Najmniejsze dopuszczalne odległości poziome lub pionowe między krawędziami kanalizacji kablowej a krawędziami linii elektroenergetycznych napowietrznych lub kablowych, a także urządzeniami odgromowymi budynków powinny być zgodne z Polskimi Normami. Na skrzyżowaniu z gazociągiem zastosować rury ochronne z rurami wydmucho.

Kanalizacja wtórna

Zaprojektowano kanalizacje wtórną mającą stanowić osłonę kabli optycznych. Kanalizacji wtórna zbudowana jest z rur RHDPE fi 32x2,9 połączonych w studniach kablowych w sposób wodo- i gazoszczelny złączkami odpornymi na działanie nadciśnienia co najmniej 1 Mpa.

Kanalizacja wtórna powinna zabezpieczać zaciągnięte do niej kable przed uszkodzeniami mechanicznymi wzdłuż całych ciągów oraz w studniach kablowych. Ciągi kanalizacji wtórnej na całej ich długości powinny być rozróżnialne. Tę rozróżnialność powinno się zapewniać przez:

- stosowanie rur z odpowiednimi napisami na zewnętrznej powierzchni,
- stosowanie rur z barwnymi wyróżnikami, jednakowymi dla poszczególnych ciągów na całej trasie kanalizacji,
- oznakowanie ciągów zajętych przez kable w studniach kablowych.

Przy zajmowaniu całego otworu kanalizacji pierwotnej dla kanalizacji wtórnej należy wciągać od razu 3 - 4 rury kanalizacji wtórnej, nawet gdyby z aktualnych potrzeb budowy wynikała konieczność zaciągania tylko jednej rury Kanalizację wtórną i trójną dzieli się na odcinki zaciągowe, których długość powinna być dostosowana do technologii zaciągania kabli lub wiązek światłowodów.

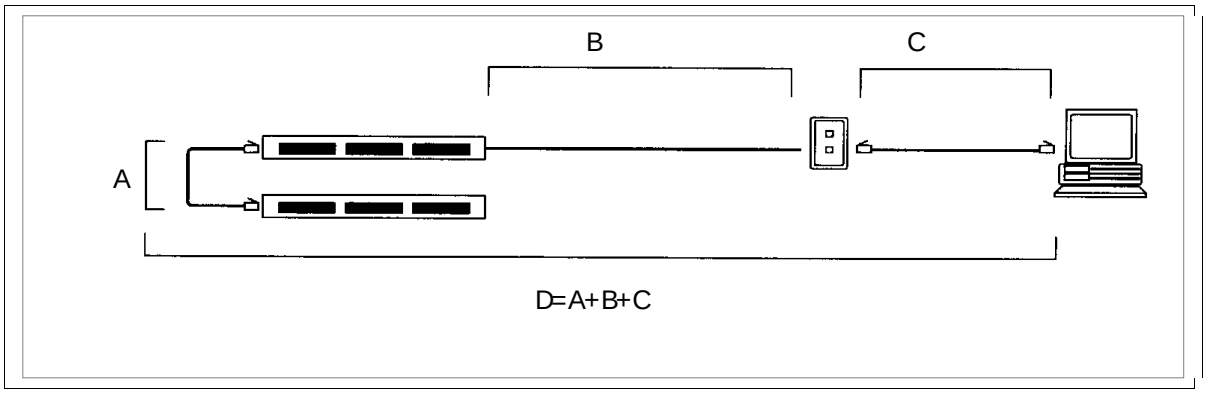
Ciągi kanalizacji wtórnej powinny być szczelne. Po wybudowaniu odcinków o długości około 2 km należy napełnić je sprężonym powietrzem i po upływie 24 godzin sprawdzić stan ciśnienia manometrem technicznym.

Kanalizacja wprowadzeniowa

Otwory kanalizacji należy uszczelnić od strony budynku oraz od strony studni kablowej. Do analizy przyjęto uszczelnienia Enco HRD w wersji dzielonej umożliwiającej uszczelnienie w przypadku dokładania lub likwidacji kabli bez konieczności demontażu kabli pracujących. Kanalizacja wprowadzeniowa powinna być zakończona w jednakowy sposób po stronie studni stacyjnej i po stronie komory kablowej. Rury kanalizacji kablowej pierwotnej powinny wystawać do 50 mm od ściany, natomiast rury kanalizacji wtórnej na co najmniej 500 mm, otwory rur pustych i z kablami powinny być uszczelnione przy pomocy uszczelek.

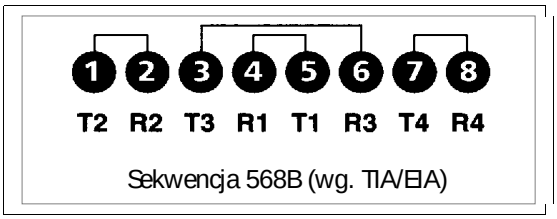
Uwagi montażowe okablowania poziomego

W okablowaniu poziomym maksymalna długość przebiegu kabla wynosi 90 m, pomiędzy interfejsem użytkownika (punkt abonencki) i panelem rozdzielczym (szafa rozdzielcza). Nie wolno w żadnym wypadku dopuścić do tego, by całkowita długość kabla pomiędzy terminalem i punktem rozdzielczym plus przyłączenie do sieciowego sprzętu komputerowego lub okablowania pionowego przekroczyła 100 m (kable krosowe, kabel przebiegu poziomego i kabel stacyjny). Maksymalna długość kabli krosowych wynosi 5 m, przy czym łączna długość kabla stacyjnego i krosowego może mieć maksymalnie 10 m.



Maksymalna długość	**Zalecana maksymalna długość**
A = Nie więcej niż 5 m	A = Nie więcej niż 5 m
A + C = 10 m (łącznie)	A + C = 10 m (łącznie)
B = 90 m	B = 60 m

Zalecaną sekwencją połączeń kabli w nowych instalacjach, w których stosuje się kable UTP/STP, jest sekwencja 568B (EIA/TIA), stosuje się tu standardowe 8-pinowe gniazdo modularne lub wtyczkę RJ45. Połączenie interfejsu modularnego z kablem jest następujące:



Sekwencja 568B (wg. TIA/EIA)

Kable powinny być wprowadzane i wyprowadzane z głównych tras przebiegu pod kątem 90^o, zaś promienie ich zgięć w kanałach powinny być zgodne z zaleceniami. Przestrzeganie tego warunku ułatwi konserwację sieci kablowej, gdyż podane kąty gwarantują łatwiejszy dostęp do kabli i szybsze zlokalizowanie przebiegów w budynku. Należy także układać kable równolegle i prostopadle do korytarzy.

Instalując kable należy zawsze sprawdzać czy nie są naprężone na końcach i na całym swoim przebiegu. Jeżeli kable znajdują się na otwartej przestrzeni, powinny być umieszczone w jednej płaszczyźnie, nie wolno owijać kabli dookoła rur, kolumn itp.

Wielkość promieni zgięć kabli w kanałach wynosi:

- W kanale o średnicy wewnętrznej do 5.1 cm (2”) lub mniejszej, promień zgięcia powinien wynosić 6-krotność tej średnicy dla kabla STP.
- W kanale o średnicy wewnętrznej 5.1 cm (2”) lub większej, a także zawierającym kable światłowodowe, promień zgięcia powinien wynosić wielokrotność dziesięciu średnicy kabla.

Uwaga ogólna: kąty zgięć kanałów rurowych nie powinny być większe niż 90^o. Jeżeli warunki zmuszają do większej ilości zgięć lub gdy trasa kanału wynosi więcej niż 30 m, wtedy należy na tej trasie przejścia zainstalować puszkę przelotową pomiędzy drugim i trzecim zgięciem (uwaga: nie w miejscu drugiego zgięcia). Z reguły tarcie wywołane przez kąt 90^o odpowiada tarciu dla 9 m prostego odcinka.

Uwagi montażowe światłowodowych

Bezpieczeństwo i higiena pracy (BHP)

Zasady ogólne

Pracownicy zatrudnieni przy budowie linii telekomunikacyjnych powinni posiadać odpowiednie przeszkolenie w zakresie BHP (wstępne, okresowe, stanowiskowe) oraz powinni otrzymać odpowiedni instruktaż na konkretnym stanowisku pracy. W dziedzinie budownictwa telekomunikacyjnego budowa, a także eksploatacja linii kablowych w kanalizacji kablowej i ziemnych, a także nadziemnych charakteryzuje się występowaniem robót o zwiększonym zagrożeniu z punktu widzenia bezpieczeństwa i higieny pracy. Z tego względu ścisłe przestrzeganie obowiązujących przepisów BHP stanowi szczególnie odpowiedzialne zadanie dla personelu nadzoru i wszystkich pracowników zatrudnionych w tej dziedzinie. Zasady BHP ujęte w odpowiednich dokumentach normatywnych obowiązują wykonawców robót oraz pracowników nadzorujących i kierujących robotami bezpośrednio i pośrednio. Pracownicy powinni znać dokładnie zasady BHP w zakresie zajmowanego stanowiska lub wykonywanych robót. Przyjęcie do wiadomości i dokładną znajomość przepisów powinien potwierdzić pracownik swoim podpisem.

Przy budowie linii telekomunikacyjnych należy w szczególności przestrzegać poniższych zasad:

a) Przy otwieraniu studni kablowej nie wolno wzruszać pokrywy włazu przez uderzanie młotkiem stalowym, oskardem itp., co może spowodować iskrzenie i ewentualny wybuch gazu. Wzruszenia pokrywy można dokonywać wyłącznie przez uderzanie drągiem drewnianym, przy równoczesnym podnoszeniu za pomocą specjalnego urządzenia do otwierania studni.

b) Rozgrzewanie otwartym płomieniem, np. palnikiem gazowym, przymarzniętej w zimie pokrywy jest bezwzględnie zabronione ze względu na możliwość wybuchu nagromadzonego w studni gazu. Dopuszcza się topienie zmarzliny przy pomocy gorącej wody lub, lepiej, strumieniem gorącego powietrza, z tym że urządzenie grzejne w wytwornicy gorącego powietrza powinno być oddalone od studni.

c) Nie wolno otwierać studni będąc z otwartym ogniem, np. zapalonym papierosem, palnikiem itp.

d) Pokrywę należy przesuwać ostrożnie, aby od uderzenia metalu o metal lub kamień nie nastąpiło iskrzenie.

e) Nie wolno schodzić do studni bezpośrednio po podniesieniu pokrywy. Schodzenie do studni musi być poprzedzone jej wietrzeniem w ciągu 10 ÷ 15 minut i równoczesnym otwarciem sąsiednich studni oraz sprawdzeniem wykrywaczem gazu, czy wewnątrz studni nie znajduje się gaz świetlny lub ziemny. Jeżeli po wywietrzeniu, po krótkim czasie gaz pojawi się ponownie, należy studnię wywietrzyć powtórnie, a przed przystąpieniem do pracy uszczelnić otwory kanalizacyjne. Niezależnie od tego, o obecności lub pojawieniu się gazu należy powiadomić właściwy terenowo zakład gazownictwa. Pracę, zwłaszcza z otwartym ogniem (palnik gazowy),

można wykonywać wyłącznie po upewnieniu się, że gazu w studni już nie ma. W czasie pracy w studniach zagrożonych gazem jeden z pracowników powinien przebywać nad studnią w celu udzielenia pomocy pracownikowi znajdującemu się w studni, jeżeli zaistnieje taka konieczność.
f) Studnie po zdjęciu pokryw należy niezwłocznie zabezpieczyć ogrodzeniami (zastawami), a w miejscach dużego ruchu kołowego (jezdnie) ustawić tablice ostrzegawcze, w nocy natomiast dobrze oświetlić światłami ostrzegawczymi
g) Przy pracy w studniach kablowych należy używać wyłącznie urządzeń oświetleniowych o napięciu do 24 V, z tym że dopuszcza się również stosowanie urządzeń oświetleniowych na napięcie 220 V w drugiej klasie izolacji.

Prace przy bębnach kablowych należy wykonywać z zachowaniem przestrzegania następujących zasad:
a) Przed rozwinięciem kabla należy bęben podnieść na kozłach (podnośnikach) kablowych na wysokość niezbędną do swobodnego obracania bębnem albo też wykorzystać przyczepę kablową.
b) Kozły powinny być ustawione na terenie równym i o twardej nawierzchni oraz w sposób uniemożliwiający poruszanie się podczas obracania bębna.
c) Przed rozpoczęciem rozwijania kabla należy z bębna usunąć wszelkie gwoździe albo je zagiąć, by nie spowodowały okaleczenia.
d) Podczas rozwijania kabla z bębna należy zwrócić uwagę, aby końcówka kabla nie odginała się od zamocowania na tarczy i nie uderzyła któregoś z robotników rozwijających kabel.
e) Przy ręcznym układaniu lub zaciąganiu kabla do kanalizacji rozstawienie robotników powinno być takie, aby ciężar przypadający na jednego robotnika nie przekraczał 30 kG.
f) Dopuszcza się przetaczanie bębnów kablowych na niewielkie odległości wyłącznie w kierunku zgodnym ze strzałką umieszczoną na tarczy bębna.
g) Donoszenie kabla powinno odbywać się ręcznie przez pracowników, przy czym wszyscy pracownicy powinni znajdować się tylko po jednej stronie kabla (zasada ta obowiązuje również przy układaniu kabla).
h) Pracownicy rozwijający, donoszący, układający lub zaciągający kabel powinni pracować w rękawicach ochronnych.

Praca z użyciem sprężarki przy pneumatycznym zaciąganiu kabli OTK do rur polietylenowych kanalizacji wtórnej lub rurociągu kablowego wymaga przestrzegania odpowiednich przepisów BHP przy urządzeniach sprężarkowych, a w szczególności:
a) Rury polietylenowe w trakcie robót należy chronić przed dostępem do nich wody, piasku, żwiru i jakichkolwiek innych przedmiotów.

b) Przed skierowaniem strumienia powietrza do rury kanalizacyjnej należy upewnić się, że jej koniec na końcu odcinka pneumatycznego jest niepowołanych i szkodliwym działaniem strumienia powietrza na otoczenie.
c) Wszystkie połączenia rur i węży należy wykonywać starannie i utrzymywać w dobrym stanie.
d) W pobliżu przewodów i urządzeń ciśnieniowych powinni przebywać tylko przeszkoleni pracownicy obsługi.
e) Przed rozpoczęciem prac każdorazowo należy przeprowadzić szczegółowy instruktaż BHP na stanowisku pracy, sprawdzić stan techniczny urządzeń, odgrodzić stanowiska pracy dla uniemożliwienia dostępu osób niepowołanych, sprawdzić poprawność działania łączności radiotelefonicznej.
f) W wypadku, gdy kabel jest zaciągany (wdmuchiwany) do rurociągu kablowego usytuowanego we wspólnym ciągu z kablami elektroenergetycznymi niskiego lub wysokiego napięcia, należy zachować szczególną ostrożność ze względu na możliwość porażenia prądem. Prace mogą być w takich sytuacjach wykonywane wyłącznie przez odpowiednio przeszkolony personel, mający wymagane uprawnienia i pracujący pod specjalistycznym nadzorem.

Zasady BHP w styczności ze światłowodami przy montażu i badaniach

Zasady ochrony przed szkodliwym promieniowaniem lasera

Promieniowanie emitowane przez diody elektroluminescencyjne, stosowane w telekomunikacji, ma małą moc i nie jest niebezpieczne. Promieniowanie emitowane przez diody laserowe stanowi zagrożenie dla oczu.

Zasady bezpieczeństwa pracy z tymi urządzeniami laserowymi określa PN-91/T-06700 *Bezpieczeństwo przy promieniowaniu emitowanym przez urządzenia laserowe. Klasyfikacja sprzętu. Wymagania i wytyczne dla użytkownika.* Zgodnie z tą normą, urządzenia laserowe muszą być oznakowane odpowiednimi etykietkami objaśniającymi i ostrzegawczymi, które informują o klasie danego urządzenia laserowego i zagrożeniu promieniowaniem laserowym. Klasa urządzenia jest określana przez producenta. Do jego obowiązków należy też umieszczenie na urządzeniu odpowiednich etykiet. Złącza światłowodów, na których wyjściu może być emitowane promieniowanie, muszą być oznakowane trójkątnym znakiem ostrzegawczym i napisem: UWAGA! - NIEWIDZIALNE PROMIENIOWANIE LASEROWE.

Urządzenia laserowe stosowane w sieci ODN należą do klasy 1, 3A lub 3B (klasa 2 dotyczy tylko promieniowania widzialnego). Urządzenia z diodami elektroluminescencyjnymi należą do klasy 1. Urządzenia klasy 1 są całkowicie bezpieczne, urządzenia klasy 3A są niebezpieczne w wypadku patrzenia na wiązkę promieniowania laserowego przez przyrządy optyczne nie

wyposażone w filtr tłumiący promieniowanie, natomiast urządzenia klasy 3B są niebezpieczne w każdym wypadku patrzenia na wiązkę promieniowania laserowego. Z tego powodu przy pracy z urządzeniami laserowymi klasy 3A i 3B jest wymagana ochrona oczu, co jest szczególnie istotne w odniesieniu do systemów OTK nie wyposażonych w układ automatycznego wyłączania lasera w wypadku awarii kabla OTK. W wypadku prowadzenia jakichkolwiek prac montażowych związanych z możliwym zagrożeniem oczu na skutek dostępu do promieniowania laserowego w urządzeniach ODN zawierających urządzenia laserowe klasy 3B, pracownicy muszą mieć założone specjalne okulary lub gogle laserowe, tłumiące promieniowanie o określonej długości fali. W wypadku urządzeń laserowych klasy 3A jest zabronione oglądanie złączy i końcówek światłowodów przy użyciu przyrządów optycznych nie wyposażonych w filtr tłumiący dane promieniowanie. Okulary i gogle laserowe oraz sprzęt optyczny do obserwacji wtyków złączy światłowodowych muszą być oznakowane w sposób trwały napisem z informacją o długości fali promieniowania, które tłumią, oraz o wielkości tego tłumienia *A*, określanego przez stosunek mocy promieniowania padającego do mocy promieniowania przechodzącego. Powyższe tłumienie *A* jest określone następująco:

A = 10 O.D.

gdzie O.D. oznacza wartość tzw. gęstości optycznej.

Tłumienie *A* równe 100 (O.D. = 2) w pełni zapewnia bezpieczeństwo oczu dla mocy promieniowania używanych w optotelekomunikacji. W szczególności należy mieć na uwadze następujące sytuacje, które mogą stwarzać zagrożenie dla wzroku w wypadku montażu i badań linii OTK stosowanych w sieci ODN:

− rozłączanie lub łączenie złączy światłowodowych w działających przełącznicach lub w działających stojakach z urządzeniami końcowymi,

− przełączanie światłowodów w węzłach złączowych i szafkowych, rozgałęziaczach światłowodów i innych obiektach działającej linii OTK,

− zgrzewanie światłowodów działających linii OTK,

− oglądanie czół lub pęknięć światłowodów oraz oglądanie złączy w działających liniach ODN lub przyrządach, np. reflektometrach.

Reasumując, w wypadku możliwości zagrożenia wzroku przy pracach w obiektach sieci ODN należy:

− spowodować wyłączenie źródła promieniowania laserowego;

− jeżeli wyłączenie źródła promieniowania laserowego nie jest możliwe, to:

• jeżeli moc promieniowania przekracza wartość klasy 1, zabrania się oglądania złączy oraz czół lub pęknięć światłowodów działających linii ODN lub przyrządów (np. reflektometrów) bez użycia

przyrządów optycznych przeznaczonych do tego celu i wyposażonych w filtr nie przepuszczający określonego promieniowania laserowego
• jeżeli moc promieniowania przekracza wartość klasy 3A, przed przystąpieniem do pracy należy założyć odpowiednio oznakowane okulary lub gogle ochronne.

Zasady ochrony przed skaleczeniem

Należy zachować szczególną ostrożność przy pracach prowadzonych w styczności ze światłowodami, gdyż ich ułamane lub odcinane końce są bardzo ostre i łatwo mogą wbijać się w skórę ludzką. Są one szczególnie niebezpieczne dla oczu, ust, skóry twarzy itp. Krótkie odcinki kabli i włókien światłowodowych powinny być starannie zbierane i składane do specjalnych pojemników, a następnie likwidowane w taki sposób, aby nie były bezpośrednio dostępne dla osób nieświadomych ich szkodliwości.

Dokumentacja powykonawcza

Dokumentacja powykonawcza wybudowanej linii kablowej (kanalizacji pierwotnej, rurociągu kablowego, linii i sieci kablowych) powinna zawierać wszystkie składniki określone w prawie budowlanym. Dokumentacja dostarczana jest inwestorowi po zakończeniu budowy.
Część trasowa dokumentacji powykonawczej powinna być sporządzona w formie odrębnego dokumentu powykonawczego, niezależnie od poprawionej dokumentacji projektowej. Powinna być ona wykonywana na bieżąco, w miarę postępu budowy, przez uprawnionego geodetę pod nadzorem wykonawcy i inspektora nadzoru. Fakt ten powinien znaleźć odzwierciedlenie w postaci odpowiedniego zapisu w dzienniku budowy.
Załącznikami do dokumentacji powykonawczej powinny być protokoły przekazania użytkownikom terenu czasowo zajętego dla potrzeb budowy oraz odpowiednie protokoły stwierdzające prawidłowość wykonania zbliżeń i skrzyżowań kanalizacji z innymi obiektami uzbrojenia terenowego.
W wypadku budowy kanalizacji wtórnej należy dokonać odpowiednich korekt i uzupełnień w dokumentacji inwentaryzacyjnej kanalizacji pierwotnej, natomiast w wypadku minikanalizacji - dokonać odpowiednich uzupełnień w dokumentacji inwentaryzacyjnej kanalizacji wtórnej, z uwzględnieniem szafek kablowych, przebiegów wewnątrz obiektów budowlanych (np. w komorach kablowych) itp.

Roboty ziemne

Roboty ziemne prowadzić przy zachowani przepisów BHP. W trakcie wykonywania robót zachować szczególną ostrożność w związku z licznie występującym uzbrojeniem podziemnym. W

celu ustalenia przebiegu tego uzbrojenia wykonać przekopy próbne prostopadłe do kierunku projektowanych linii kablowych. W trakcie prowadzenia robót nie uszkodzić systemu korzennego drzew.

Zestawienie materiałów okablowania strukturalnego

Na potrzeby projektu rozważano przykładowe materiały na bazie produktów Reichle&de Massari. Można zastosować inne produkty o nie gorszych parametrach, właściwościach i jakości niż zaprojektowane. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Nr. Kat.	Opis produktu	Ilość
	Szafa przyłącza	
R112817	Szafa SZB 19" 42U 800x800 z drzwiami przednimi szklanymi lub równoważne rozwiązanie	1
R112168	Cokół zwykły 100x800x800mm lub równoważne rozwiązanie	1
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	1
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	1
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	2
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	4
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	4
R512417	PP HD-19" 1U-48xRJ45-C6A ISO/s- lub równoważne rozwiązanie	1
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	4
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	1
R509858	Pa-C6As-1-gu-st-rj45s-st-rj45s-a-1.0 lub równoważne rozwiązanie	48
R112020-3DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; MM50um; OM3 dł.1m lub równoważne rozwiązanie	8
R112020-9DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; SM 9um; J G652 dł.1m lub równoważne rozwiązanie	8
	LOT GPD	
R113173	Szafa serwerowa SE 19" 42U 600x1000 z cokołem 100mm lub równoważne rozwiązanie	3
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	3
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	3

R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	3
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	2
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	2
R512417	PP HD-19" 1U-48xRJ45-C6A ISO/s- lub równoważne rozwiązanie	2
R512419	PP HD-19" 1U-24xRJ45-C6A ISO/s- lub równoważne rozwiązanie	1
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	5
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R512760	HDS Level 3-Plug Guard Key- lub równoważne rozwiązanie	1
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R508117	Key for Plug Guard LC-D connector lub równoważne rozwiązanie	1
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	102
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	51
R310786	WM Global Outlet, 80x80,2x1 Port lub równoważne rozwiązanie	4

LOT LPD1

R112817	Szafa SZB 19" 42U 800x800 z drzwiami przednimi szklanymi lub równoważne rozwiązanie	1
R112168	Cokół zwykły 100x800x800mm lub równoważne rozwiązanie	1
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	1
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	1
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	1
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	1
R512426	MH HD-4x 12x /s- lub równoważne rozwiązanie	2
R510088	Module RJ45/s C6A-ISO-sp-100 lub równoważne rozwiązanie	24
R512417	PP HD-19" 1U-48xRJ45-C6A ISO/s- lub równoważne rozwiązanie	4
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	6
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	164
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	80
R310786	WM Global Outlet, 80x80,2x1 Port lub równoważne rozwiązanie	4

LOT LPD2

R112817	Szafa SZB 19" 42U 800x800 z drzwiami przednimi szklanymi lub równoważne rozwiązanie	1
R112168	Cokół zwykły 100x800x800mm lub równoważne rozwiązanie	1
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	1
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	1
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	1
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	1
R512426	MH HD-4x 12x /s- lub równoważne rozwiązanie	2
R510088	Module RJ45/s C6A-ISO-sp-100 lub równoważne rozwiązanie	24
R512417	PP HD-19" 1U-48xRJ45-C6A ISO/s- lub równoważne rozwiązanie	1
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	2
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	59
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	27
R310786	WM Global Outlet, 80x80,2x1 Port lub równoważne rozwiązanie	5

LOT Kable

R304143	LT-cable-indoor-4-os1 cena jedn. za 1km lub równoważne rozwiązanie	0,2
R308217	LT-cable-indoor-4-om3 cena jedn. za 1km lub równoważne rozwiązanie	0,2
R305649	Real10 S/FTP 4P 650 MHz LSZH op.500m cena jedn. za 1km lub równoważne rozwiązanie	22
R509858	Pa-C6As-1-gu-st-rj45s-st-rj45s-a-1.0 lub równoważne rozwiązanie	408
R112020-3DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; MM50um; OM3 dł.1m lub równoważne rozwiązanie	8
R112020-9DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; SM 9um; J G652 dł.1m lub równoważne rozwiązanie	8

SC

SC GPD

R113173	Szafa serwerowa SE 19" 42U 600x1000 z cokołem 100mm lub równoważne rozwiązanie	2
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	2
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	2

R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	2
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	1
R512426	MH HD-4x 12x /s- lub równoważne rozwiązanie	2
R510088	Module RJ45/s C6A-ISO-sp-100 lub równoważne rozwiązanie	24
R512419	PP HD-19" 1U-24xRJ45-C6A ISO/s- lub równoważne rozwiązanie	1
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	2
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	24
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	12

SC LPD1

R112817	Szafa SZB 19" 42U 800x800 z drzwiami przednimi szklanymi lub równoważne rozwiązanie	1
R112168	Cokół zwykły 100x800x800mm lub równoważne rozwiązanie	1
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	1
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	1

Nr. Kat.	Opis produktu	Ilość
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	1
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	1
R512426	MH HD-4x 12x /s- lub równoważne rozwiązanie	2
R510088	Module RJ45/s C6A-ISO-sp-100 lub równoważne rozwiązanie	24
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	1
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	8
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	4

SC kable lub równoważne rozwiązanie

R304143	LT-cable-indoor-4-os1 cena jedn. za 1km lub równoważne rozwiązanie	0,1
R308217	LT-cable-indoor-4-om3 lub równoważne rozwiązanie	0,1
R305649	Real10 S/FTP 4P 650 MHz LSZH op.500m lub równoważne rozwiązanie	2,5

R509858	Pa-C6As-1-gu-st-rj45s-st-rj45s-a-1.0 lub równoważne rozwiązanie	72
R112020-3DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; MM50um; OM3 dł.1m lub równoważne rozwiązanie	4
R112020-9DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; SM 9um; J G652 dł.1m lub równoważne rozwiązanie	4

SG

SG GPD

R113173	Szafa serwerowa SE 19" 42U 600x1000 z cokołem 100mm lub równoważne rozwiązanie	2
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	2
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	2
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	2
R512416	PP HD-19" 1U-empty	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	1
R512426	MH HD-4x 12x /s- lub równoważne rozwiązanie	2
R510088	Module RJ45/s C6A-ISO-sp-100 lub równoważne rozwiązanie	24
R512419	PP HD-19" 1U-24xRJ45-C6A ISO/s- lub równoważne rozwiązanie	1
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	2
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	28
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	14

SG LPD1

R112817	Szafa SZB 19" 42U 800x800 z drzwiami przednimi szklanymi lub równoważne rozwiązanie	1
R112168	Cokół zwykły 100x800x800mm lub równoważne rozwiązanie	1
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	1
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	1
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	1
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	1
R512426	MH HD-4x 12x /s- lub równoważne rozwiązanie	2

R510088	Module RJ45/s C6A-ISO-sp-100 lub równoważne rozwiązanie	24
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	1
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	14
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	7

SG kable

R304143	LT-cable-indoor-4-os1 cena jedn. za 1km lub równoważne rozwiązanie	0,1
R308217	LT-cable-indoor-4-om3 cena jedn. za 1km lub równoważne rozwiązanie	0,1
R305649	Real10 S/FTP 4P 650 MHz LSZH op.500m cena jedn. za 1km lub równoważne rozwiązanie	3
R509858	Pa-C6As-1-gu-st-rj45s-st-rj45s-a-1.0 lub równoważne rozwiązanie	72
R112020-3DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; MM50um; OM3 dł.1m lub równoważne rozwiązanie	4
R112020-9DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Du plex; kabel duplex 2,0mm; SM 9um; J G652 dł.1m lub równoważne rozwiązanie	4

SOL

SOL GPD

R113173	Szafa serwerowa SE 19" 42U 600x1000 z cokołem 100mm lub równoważne rozwiązanie	3
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	3
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	3
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	3
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	2
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	2
R512417	PP HD-19" 1U-48xRJ45-C6A ISO/s- lub równoważne rozwiązanie	2
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	3
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	80
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	40

SOL LPD1

R112817	Szafa SZB 19" 42U 800x800 z drzwiami przednimi szklanymi lub równoważne rozwiązanie	1
R112168	Cokół zwykły 100x800x800mm lub równoważne rozwiązanie	1
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	1
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	1
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	1
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	1
R512426	MH HD-4x 12x /s- lub równoważne rozwiązanie	2
R510088	Module RJ45/s C6A-ISO-sp-100 lub równoważne rozwiązanie	24
R512417	PP HD-19" 1U-48xRJ45-C6A ISO/s- lub równoważne rozwiązanie	3
R502272	CM 1U 19" Metal Panel, Modular 70mm lub równoważne rozwiązanie	4
R512757	HDS Level 3-Plug Guard-gn lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector lub równoważne rozwiązanie	8
R509504	Module RJ45/s C6A ISO-fr lub równoważne rozwiązanie	144
R313332	Mounting Plate 45x45 mm, angled, white lub równoważne rozwiązanie	72

SOL LPD2

R112817	Szafa SZB 19" 42U 800x800 z drzwiami przednimi szklanymi lub równoważne rozwiązanie	1
R112168	Cokół zwykły 100x800x800mm lub równoważne rozwiązanie	1
R113690	Panel wentylacyjny dachowy PWD-4W 380x380mm z 4 wentylatorami lub równoważne rozwiązanie	1
R112073	Termostat KTS 1141 (zamykający) lub równoważne rozwiązanie	1
R112074	Listwa zasilająca LZ-30F 440mm z 5 gniazdami 2P+Z z filtrem sieciowym 30MHz lub równoważne rozwiązanie	1
R512416	PP HD-19" 1U-empty lub równoważne rozwiązanie	1
R808374	FiberModul HD, splice, 6xLC-Duplex G.652.D, PC, ceramic, C/2 lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic lub równoważne rozwiązanie	1
R512426	MH HD-4x 12x /s- ceramic lub równoważne rozwiązanie	2
Nr. Kat.	Opis produktu	Ilość
R510088	Module RJ45/s C6A-ISO-sp-100 ceramic lub równoważne rozwiązanie	24
R512417	PP HD-19" 1U-48xRJ45-C6A ISO/s- ceramic lub równoważne rozwiązanie	1
R502272	CM 1U 19" Metal Panel, Modular 70mm ceramic lub równoważne rozwiązanie	2
R512757	HDS Level 3-Plug Guard-gn ceramic lub równoważne rozwiązanie	8
R508116	Plug Guard for LC-D connector ceramic lub równoważne	8

	rozwiązanie	
R509504	Module RJ45/s C6A ISO-fr ceramic lub równoważne rozwiązanie	44
R313332	Mounting Plate 45x45 mm, angled, white ceramic lub równoważne rozwiązanie	22
	SOL Kable	
R304143	LT-cable-indoor-4-os1 cena jedn. za 1km ceramic lub równoważne rozwiązanie	0,1
R308217	LT-cable-indoor-4-om3 cena jedn. za 1km ceramic lub równoważne rozwiązanie	0,1
R305649	Real10 S/FTP 4P 650 MHz LSZH op.500m cena jedn. za 1km ceramic lub równoważne rozwiązanie	17
R509858	Pa-C6As-1-gu-st-rj45s-st-rj45s-a-1.0 ceramic lub równoważne rozwiązanie	336
R112020-3DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; MM50um; OM3 dł.1m ceramic lub równoważne rozwiązanie	8
R112020-9DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; SM 9um; J G652 dł.1m ceramic lub równoważne rozwiązanie	8
	CCTV	
R304143	LT-cable-indoor-4-os1 cena jedn. za 1km ceramic lub równoważne rozwiązanie	0,3
R305649	Real10 S/FTP 4P 650 MHz LSZH op.500m cena jedn. za 1km ceramic lub równoważne rozwiązanie	7,5
R512416	PP HD-19" 1U-empty ceramic lub równoważne rozwiązanie	1
R515091	FiberModul HD, splice, 6xLC-Duplex OM3, PC, ceramic ceramic lub równoważne rozwiązanie	2
R512426	MH HD-4x 12x /s- ceramic lub równoważne rozwiązanie	2
R510088	Module RJ45/s C6A-ISO-sp-100 ceramic lub równoważne rozwiązanie	24
R512417	PP HD-19" 1U-48xRJ45-C6A ISO/s- ceramic lub równoważne rozwiązanie	2
R502272	CM 1U 19" Metal Panel, Modular 70mm ceramic lub równoważne rozwiązanie	3
R310786	WM Global Outlet, 80x80,2x1 Port ceramic lub równoważne rozwiązanie	114
R509504	Module RJ45/s C6A ISO-fr ceramic lub równoważne rozwiązanie	114
R509496	Hybrid-Outlet-2/1-lcd-z-apc-no-c ceramic lub równoważne rozwiązanie	6
R509857	Pa-C6As-1-gu-st-rj45s-st-rj45s-a-0.5 ceramic lub równoważne rozwiązanie	114
R112020-3DLDLD001	Patchcord ze złączami LC/PC Duplex-LC/PC Duplex; kabel duplex 2,0mm; MM50um; OM3 dł.1m ceramic lub równoważne rozwiązanie	6

Zestawienie materiałów kanalizacji teletechnicznej pierwotnej

Podano przykładowe materiały przyjęto do analziy na potrzerby projektu. Można zastosować inne produkty o nie gorszych parametrach, właściwościach i jakości niż zaprojektowane.

LP	opis	jm	ilość
1	studnia SKMP-3	szt.	1
2	studnia SKR-2	szt.	3
3	studnia SK2	szt.	5
4	rury HDPE fi 110mm gładkościenne na potrzeby projektu rozważano AROT SRS-G110/6,3 lub równoważne.	m	450

Zestawienie materiałów okablowania światłowodowego CCTV

Podano przykładowe materiały. Można zastosować inne produkty o nie gorszych parametrach, właściwościach i jakości niż zaprojektowane.

LP	opis	jm	ilość
1	rury kanalizacji wtórnej na potrzeby projektu rozważano OPTEL RHDPE 25 lub rónoważne	m	754
2	mediakonwenter na potrzeby projektu rozważano Media konwerter TP-LINK MC111CS - 100 Mb/s, jednomodowy, SC, do 20 km Tx:1550 nm Rx:1310 nm lub równowane	szt.	12

Pozostałe materiały w sieci strukturalnej.

Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Urządzeni aktywne sieci komputerowych i łączność

Wstęp – założenia projektu

Przedmiotem opracowania jest koncepcja sieci komputerowej LAN dla potrzeb terminala pasażerskiego w zakresie warstwy logicznej i zastosowanych urządzeń aktywnych oraz systemu telekomunikacyjnego telefonii VoIP.

Do analizy projekotwejy przyjęto rozwiązania typów urządzeń. Można użyć innych typów równważnych spełniających przyjete i podane w domumentacji projekotwej parametry techncizne.

Celem projektowanej instalacji jest zapewnienie wydajnej, bezpiecznej i niezawodnej transmisji danych w lokalnej sieci komputerowej Portu Lotniczego Mazury. Można zastosować elementy równoważne pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż przyjęte w projekcie.

Ze względu na konieczność pracy 4 niezależnych służb na terenie lotniska planuje się wykonanie 4 odrębnych sieci połączonych przez bezpieczny moduł styku. Niezależnie od tych sieci zaprojektowana zostanie wydzielonona fizycznie sieć obsługująca systemy BMS.

Założono, ze projektowana sieć spełniać będzie następujące wymagania funkcjonalne:

1. Bezpieczeństwo
2. Niezawodność
3. Łatwość rozbudowy o nowe aplikacje
4. Łatwość zarządzania
5. Wysoka wydajność

Infrastruktura musi posiadać możliwości obsługi wielu grup użytkowników (multi-client)

Dodatkowe usługi takie jak telefonia VoIP z priorytetyzacją ruchu (QoS) i dostęp do Internetu musza być udostępnione dla każdej z tych grup. Poszczególni użytkownicy mogą być dołączani w każdym z punktów sieci. Poszczególne sieci muszą być odizolowane fizycznie i logicznie od pozostałych sieci na terenie obiektu i połączone jedynie poprzez bezpieczny moduł styku.

W momencie dołączania do sieci, musi następować uwierzytelnienie użytkownika.

Wszystkie maszyny włączane do sieci powinny być skanowane w celu uniknięcia dołączania maszyn zainfekowanych wirusami lub posiadających wersje systemów operacyjnych szczególnie narażonych na ataki hakerów (bez aktualnych poprawek).

System musi zapewniać skuteczną ochronę przed próbami włamań

System zarządzania musi pozwalać na łatwe i pewne przydzielanie dozwolonych przez politykę bezpieczeństwa usług i aplikacji do poszczególnych sieci logicznych, grup użytkowników, adresów IP/MAC i fizycznych portów na przełączniku.

Jako podstawę rozmieszczenia urządzeń aktywnych oraz standardu połączeń pomiędzy nimi przyjęto projekt systemu okablowania strukturalnego. Tabela nr 1 poniżej przedstawia ilości gniazd okablowania dla poszczególnych sieci.

Punkt dystrybucyjny	Szafa/sieć	ilość gniazd w okablowaniu strukturalnym,	ilość portów w przełącznikach (50%) gniazd LAN, 100% WLAN)	razem portów w przełącznikach dla danej szafy	kondygnacja	Przełączniki dostępowe model	ilość	miejsce [U]*	moc (W)*	I max [A]*	ciepło tracone BTU/h*
GPD	LOT	2x20	20		P1						
			4		PP	B5K125-48P2	1	1	500	7,5A	427
		2x31	31	55	PP	B5K125-24P2	1	1	423	7,5A	335
	SC	2x6	6		P1						
		2x6	6	12	P1	B5G124-24P2	1	1	468	7,5A	318
	SG	2x8	8		P1						
		2x6	6	14	PP	B5G124-24P2	1	1	468	7,5A	318
	SOL	2x8	8		P1						
		2x32	32	40	PP	B5K125-48P2	1	1	500	7,5A	427
LPD1	LOT	2x80	80		PP						
				80	PP	B5K125-48P2	2	1	500	7,5A	427
	SC	4x2	4		PP	B5G124-24P2	1	1	468	7,5A	318
	SG	7x2	7	11	PP	B5G124-24P2	1	1	468	7,5A	318
	SOL	2x72	72	72	PP	B5K125-48P2	2	1	500	7,5A	427

Punkt dystrybucyjny	Szafa/sieć	ilość gniazd w okablowaniu strukturalnym,	ilość portów w przełącznikach (50%) gniazd LAN, 100% WLAN)	razem portów w przełącznikach dla danej szafy	kondygnacja	Przełączniki dostępowe model	ilość	miejsce [U]*	moc (W)*	I max [A]*	ciepło tracone BTU/h*
LPD2	LOT	2x14	14		P1						
		2x13	13	27	PP	B5K125-24P2	1	1	423	7,5A	335
	SOL	2x8	8		PP						
		2x14	14	22	PP	B5K125-24P2	1	1	423	7,5A	335

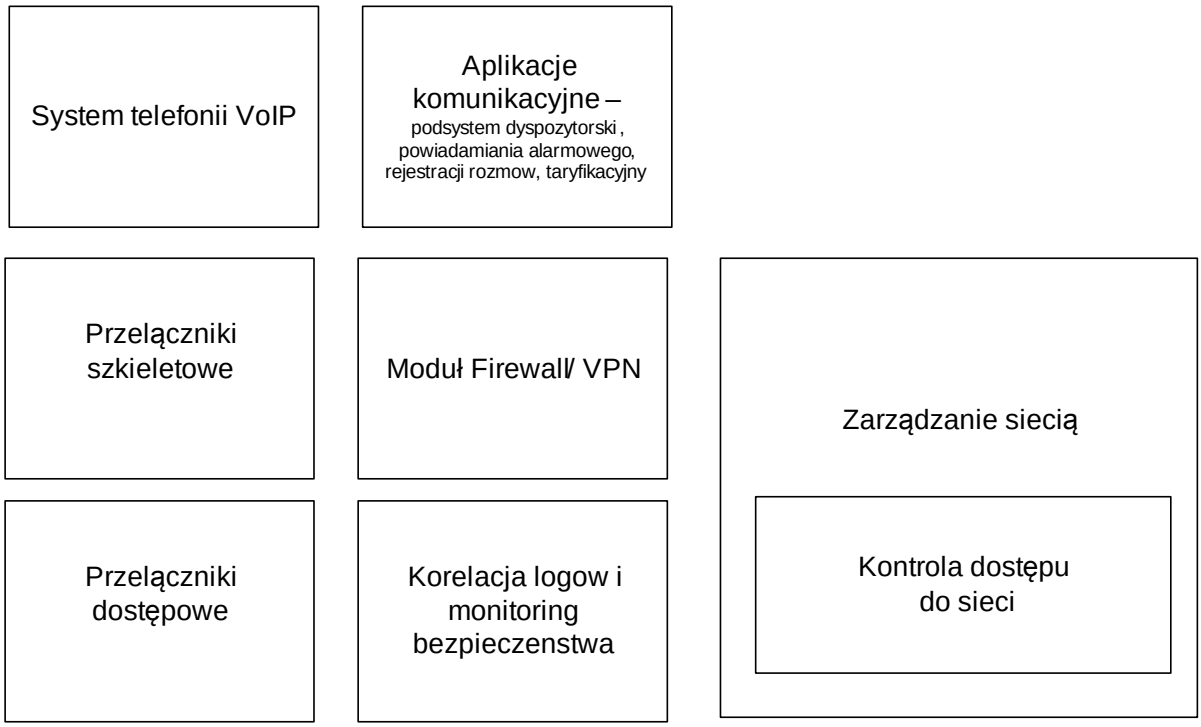
* na jeden przełącznik

Urządzenia aktywne sieci LAN

Moduły funkcjonalne

Projekt systemów sieci LAN został podzielony na moduły funkcjonalne i obejmuje kolejno:

1. Przełączniki szkieletowe
2. Przełączniki dostępowe
3. Moduł bezpiecznej komunikacji między sieciami poszczególnych służb i dostępu do Internetu (Firewall)
4. Moduł zarządzania i kontroli dostępu do sieci
5. Moduł korelacji zdarzeń bezpieczeństwa
6. System telefonii VoIP
7. Aplikacje komunikacyjne



Rysunek 1 Moduły funkcjonalne uwzględnione w projekcie

Topologia sieci LAN

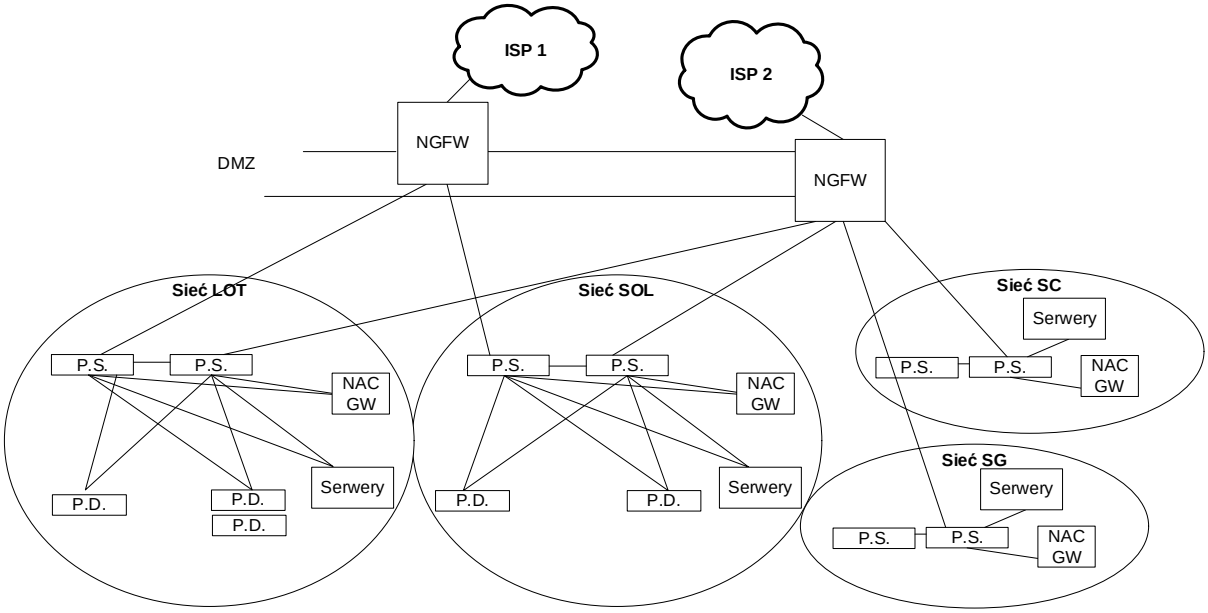
W odniesieniu do przyjętych założeń projektowych i wymagań funkcjonalnych projektowana sieć LAN będzie posiadać architekturę dwuwarstwową, w której funkcje szkieletu (core) sieci będą realizowane na urządzeniach realizujących równocześnie funkcje warstwy dystrybucyjnej. Urządzenia te będą odpowiedzialne zarówno za maksymalnie efektywne przełączanie i routowanie pakietów oraz zapewnienie funkcji filtrowania ruchu, funkcji związanych z obsługą QoS itp. Ze względu na wymóg realizacji czterech niezależnych sieci, zaprojektowane zostały dedykowane sieciowe urządzenia aktywne do obsługi każdej z sieci. Urządzenia dobrano tak, aby odsłużyć wszystkie projektowane przyłącza sieciowe okablowania strukturalnego.

Ze względu na wielkość sieci nie przewiduje się oddzielnych przełączników do obsługi farmy serwerów, a ruch z data center będzie obsługiwany bezpośrednio przez przełączniki szkieletowe.

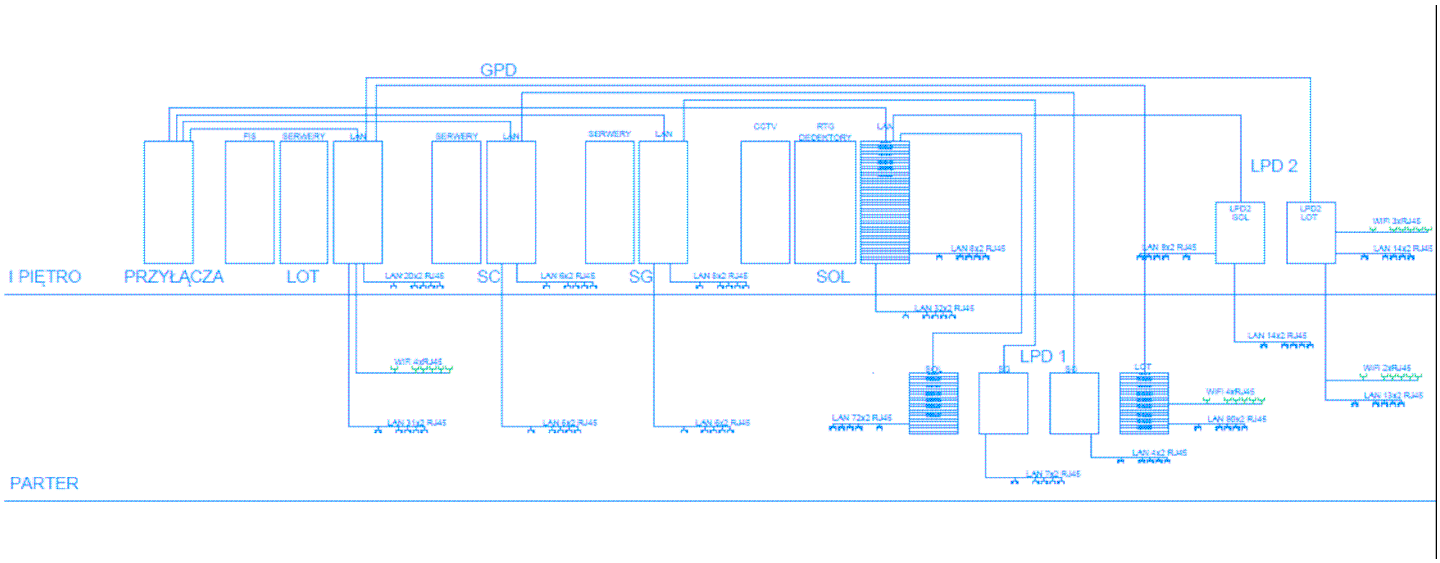
W przypadku dwóch sieci o bardzo małej liczbie portów dostępowych (sieć służby celnej - SC i sieć straży granicznej - SG, zrezygnowano z topologii dwuwarstwowej, projektując dla każdej z tych sieci po jednym przełączniku 24 portowym w punkcie dystrybucyjnym oraz po jednym przełączniku 24 na parterze oraz w serwerowi na 1 piętrze. Przełączniki zainstalowane w serwerowni na I piętrze obsługiwać będą zarówno porty dostępowe z rejonu I piętra, jak i porty lokalnych serwerów dla sieci odpowiednio służby celnej i straży granicznej)

Utworzony zostanie logiczny blok urządzeń odpowiedzialnych za komunikację z

Internetem oraz komunikację pomiędzy trzema niezależnymi sieciami, oraz zabezpieczenie tego rodzaju ruchu. Dostęp do Internetu chroniony będzie przez parę urządzeń typu Next Generation Firewall (NGFW) integrujących funkcje firewall i IPS w jednym urządzeniu .



Rysunek 2 Topologia sieci komputerowych portu lotniczego



Rysunek 3 Rozmieszczenie szaf w poszczególnych punktach dystrybucyjnych

Przełączniki dostępowe

Urządzenia warstwy dostępowej udostępniają porty do podłączenia terminali końcowych użytkowników (komputerów PC/telefonów VoIP itp.).Jednym z głównych zadań tych urządzeń w nowoczesnej sieci LAN jest filtracja i separacja ruchu już na samym brzegu sieci, dzięki czemu zasoby sieci są wykorzystywane tylko do obsługi ruchu, który jest w niej pożądany. Wszelki ruch niepożądany (wynikający z błędnej konfiguracji terminala końcowego, niezgodny z polityką bezpieczeństwa czy też po prostu będący atakiem, będzie odrzucany już na samym brzegu sieci. Jednocześnie dzięki szczegółowej informacji dotyczącej kategorii danego ruchu aż do poziomu aplikacji, sieć pozwala na indywidualne przydzielanie zasobów dla poszczególnych kategorii ruchu per użytkownik, co pozwoli na przejrzyste i wydajne zarządzanie bezpieczeństwem sieci. Polityki bezpieczeństwa są szczegółowymi regułami pozwalającymi na określanie zasobów sieci (dopuszczalnego ruchu, dozwolonych aplikacji i reguł QoS) wykorzystywanych indywidualnie przez każdego użytkownika. Dzięki zastosowaniu tego mechanizmu przy zdecydowanie mniejszym nakładzie pracy niż przy tradycyjnym wykorzystaniu list ACL osiągnięta zostanie dużo większa kontrola i bezpieczeństwo w sieci.

Przełączniki dostępowe będą pełnić ważną funkcję w rozproszonym systemie IPS. W przypadku wykrycia zagrożenia, jego źródło może zostać wyeliminowane przez automatyczną zmianę reguł (polityki bezpieczeństwa) na porcie dostępowym przełącznika, do którego jest podłączone.

Warstwę dostępową stanowią przełączniki w punktach dystrybucyjnych LPD , w których zlokalizowane są punkty zbiegu okablowania strukturalnego. Przełączniki warstwy dostępowej muszą mieć możliwość montażu w szafie 19”. Przełączniki muszą zapewniać zasilanie PoE w standadzie 802.1at poprzez okablowanie UTP, dla zasilania terminali końcowych w szczególności telefonów systemu telefonii VoIP. Przewidywane dla warstwy dostepowej przełączniki to urządzenia stakowalne o wysokości 1U, wymaga się aby stakowanie(łączenie w stosy widoczne dla zarządzania jaki jeden logiczny przełącznik) przełączników realizowane było na bazie dedykowanych do tego celu portów. Przełączniki dostępowe będą połączone ze szkieletem sieci za pomocą redundantnych uplinków 10 Gb/s.

Można zastosować rónoważne elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż przyjęte w projekcie.

Punkt dystrybucyjny	Szafa/sieć	ilość gniazd w okablowaniu strukturalnym,	ilość portów w przełacznikach (50%) gniazd LAN, 100% WLAN)	razem portów w przełącznikach dla danej szafy	kondygnacja	Przełączniki dostępowe model	ilość	miejsce [U]*	moc (W)*	I max [A]*	ciepło tracone BTU/h*
GPD	LOT	2x20	20		P1						
			4		PP	B5K125-48P2	1	1	500	7,5A	427
		2x31	31	55	PP	B5K125-24P2	1	1	473	7,5A	335
	SC	2x6	6		P1						
		2x6	6	12	P1	B5K125-24P2	1	1	473	7,5A	335
	SG	2x8	8		P1						
		2x6	6	14	PP	B5K125-24P2	1	1	473	7,5A	335
	SOL	2x8	8		P1						
		2x32	32	40	PP	B5K125-48P2	1	1	500	7,5A	427
LPD1	LOT	2x80	80		PP						
		wifi	4	84	PP	B5K125-48P2	2	1	500	7,5A	427
	SC	4x2	4		PP	B5K125-24P2	1	1	473	7,5A	335
	SG	7x2	7	11	PP	B5K125-24P2	1	1	473	7,5A	335
	SOL	2x72	72	72	PP	B5K125-24P2	1	1	473	7,5A	335
						B5K125-48P2	1	1	500	7,5A	427
LPD2	LOT	2x14	14		P1						
		2x13	13		PP						
			2		PP						
			3	32	P1	B5K125-48P2	1	1	500	7,5A	427
	SOL	2x8	8		PP						
		2x14	14	22	PP	B5K125-24P2	1	1	473	7,5A	335

* na jeden przełącznik

Przełączniki zastosowane w roli przełączników dostępowych spełniać muszą następujące minimalne wymagania:

- Posiadać (w zależności od miejsca instalacji – patrz wymagania ilościowe) 48 lub 24 porty10/100/1000 oraz 2 porty 10GbE SFP+ oraz 2 porty umożliwiające łączenie w stos (wieżę) lub 24 porty 10/100/1000 (w tym 2 combo SFP)
- Przełączniki wspierające 802.3af lub 802.3at Power over Etnernet (PoE), muszą mieć możliwość dołączenia do stosu z przełącznikami nie obsługującymi PoE.
- Musi zapewniać przełączanie z pełną prędkością łącza
- Musi obsługiwać IP Multicast
- Musi obsługiwać COS Inbound Rate Limiting per Policy User
- Musi obsługiwać 802.1p Traffic Classification
- Musi posiadać możliwości klasyfikowania pakietów warstw 2/3/4, które mogą opierać się na ID portu fizycznego, adresie MAC, podsieci IP, adresie IP, typie protokołu IP, IP ToS (Type of Service), DSCP (Differentiated Services Code Point) oraz porcie TCP/UDP.
- Musi obsługiwać IP ToS Rewrite
- Musi obsługiwać Weighted Round Robin i Strict Priority Queuing
- Musi obsługiwać do 8 priorytetowych kolejek na port
- Musi obsługiwać IEEE 802.3ad Link Aggregation
- Musi zapewniać dystrybucję zagregowanych linków pomiędzy wieloma przełącznikami w obrębie stosu
- Musi umożliwiać tworzenie stosów w formie zamkniętej pętli.
- Minimalna wydajność matrycy stakującej 50Gbps
- Wydajność przełączania minimum 72 Mpps/ 96Gbps
- Musi zapewniać redundantne zarządzanie stosem.
- Musi umożliwiać zarządzanie stosem przy wykorzystaniu jednego adresu IP.
- Musi posiadać opcjonalne, redundantne źródło zasilania.
- Musi obsługiwać uwierzytelnianie użytkownika poprzez IEEE 802.1x
- Musi obsługiwać uwierzytelnianie wykorzystujące adres MAC
- Musi obsługiwać uwierzytelnianie wykorzystujące przeglądarkę internetową
- Musi umożliwiać uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC,
- Musi obsługiwać MAC Port Locking (dynamiczne i statyczne)
- Musi obsługiwać Dynamic VLAN Assignment (RFC 3580)
- Musi obsługiwać wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet

- Musi mieć możliwość przypisania uprawnień od warstwy 2 do 4. Zapewniając ciągłe zarządzanie tożsamością wraz z funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma.
- Musi zapewniać bezpieczne zarządzanie przy wykorzystaniu: SSH, SSL, SNMPv3, RADIUS oraz TACACS+. Obsługa TACACS+ musi zapewniać wsparcie dla procesów uwierzytelniania, autoryzacji i audytowania.
- Musi obsługiwać opcje Secure Copy oraz Secure FTP
- Musi zapewniać ochronę przed atakami typu DHCP/ARP spoofing/snooping.
- Musi dostarczać ostrzeżenia o wysokiej temperaturze przez komunikaty SNMP traps oraz zdarzenia syslog.
- Musi zapewnić monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP.
- Musi obsługiwać następujące grupy RMON: Statistics, History, Alarms, Events, Packet Capture/Filtering Sampling
- Musi obsługiwać sFlow lub równoważne
- Musi obsługiwać Port Mirroring
- Musi obsługiwać IEEE 802.1s Multiple Spanning Tree
- Musi obsługiwać IEEE 802.1w Rapid Reconfiguration of Spanning Tree
- Musi obsługiwać IGMP Snooping (v1, v2, v3)
- Musi obsługiwać do 4,096 ID sieci VLAN oraz do 1,024 VLAN aktywnych jednocześnie w pojedynczym stosie
- Pojemność tablicy MAC minimum 30000 adresów
- Musi obsługiwać sieci VLAN IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP lub równoważne
- Musi obsługiwać LLDP / LLDP-MED Network-Policy TLV
- Musi obsługiwać Jumbo Ethernet Frames
- Musi zapewniać prosty routing IP (trasy statyczne oraz RIP v1/v2)
- Musi umożliwiać wykrywanie lokalizacji systemów końcowych w czasie rzeczywistym i przechowywanie tych informacji w centralnej bazie danych
- Musi działać w temperaturze otoczenia do 50°C

Przełączniki szkieletowe

Jako przełączniki szkieletowe dla sieci LOT zastosowane zostaną wydajne przełączniki modularne co najmniej czteroslotowe,o wysokości maksimum 11U i wydajności przełączania, co najmniej 640Gb/s dla warstwy 2 i co najmniej 480 Mpps dla warstwy 3.

Jako przełączniki szkieletowe dla sieci SOL zastosowane zostaną wydajne przełączniki jednomodułowe 2U o wydajności przełączania, co najmniej 640Gb/s dla warstwy 2 i co najmniej 480 Mpps dla warstwy 3.
Sieci SD, SC oraz wydzielona sieć BMS zostaną zrealizowane jako sieci jednowarstwowe z wykorzystaniem takich samych przełączników jak dla warstwy dystrybucyjnej pozostałych sieci.

Przełączniki szkieletowe (LOT,SOL) muszą posiadać zdolność do zbierania danych typu NetFlow z prędkością wire-speed, bez utraty wydajności lub konieczności stosowania technik próbkowania dla uzyskania pełnego podglądu wykorzystania zasobów sieciowych przez użytkowników i aplikacje.

Punkt dystrybucyjny	Szafa/sieć	Moduł	Opis	ilość	miejsce [U]*	moc (W)*	I max [A]*	ciepło tracone BTU/h*
GPD	LOT	S4-CHASSIS	S-Series S4 Chassis and fan tray (Power supplies ordered separately)	2	9	471	2x20A	1935
		SK5208-0808-F6	S-Series S155 Class I/O-Fabric Module, 1280Gbps Load Sharing - 8 Ports 10GBASE-X via SFP+ and two Type2 option slots (Used in S1/S4/S6/S8)	2				
		SOT2206-0112	S-Series Option Module (Type1) - 12 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) (Compatible with Type1 & Type2 option slots)	2				

Punkt dystrybucyjny	Szafa/sieć	Moduł	Opis	ilość	miejsce [U]*	moc (W)*	I max [A]*	ciepło tracone BTU/h*
		S-AC-PS	S-Series AC power supply, 20A, 100-240VAC input, (1200/1600W) (For use w/ S3/S4/S6/S8)	4				
	SOL	S1-CHASSIS-A	S-Series S1 Chassis and fan tray. Compatible with Fabric Modules only. (SSA 1000W Power supplies ordered separately)	2	2	723	2*15A	3024
		SK5208-0808-F6	S-Series S155 Class I/O-Fabric Module, 1280Gbps Load Sharing - 8 Ports 10GBASE-X via SFP+ and two Type2 option slots (Used in S1/S4/S6/S8)	2				
		SOT2206-0112	S-Series Option Module (Type1) - 12 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) (Compatible with Type1 & Type2 option slots)	2				
		SSA-AC-PS-1000W	S-Series Standalone (SSA S130 and SSA150 Class) and S1 Chassis - AC and PoE power supply, 15A, 110-240VAC input, (1000/1200W)	2				

Przełączniki muszą realizować uwierzytelnianie wielu użytkowników przy wykorzystaniu wielu metod na każdym porcie przełącznika – jest to absolutnie niezbędne, gdy do sieci podłączone są takie urządzenia jak telefony IP, komputery, drukarki, kserokopiarki, kamery bezpieczeństwa, czytniki kart identyfikacyjnych lub maszyny wirtualne.
Para przełączników szkieletowych dla każdej z sieci LOT i SOL połączona zostanie za pomocą technologii VSB – virtual chassis bonding w jedno urządzenie wirtualne. Dzięki takiemu rozwiązaniu uproszczona zostanie logiczna topologia sieci i wyeliminowana potrzeba zastosowania protokołu STP. Eliminacja protokołu STP pozwoli na pełne wykorzystanie redundantnych uplinków, gdyż przełącznik wirtualny będzie mógł realizować agregację linków na interfejsach fizycznie znajdujących się w dwóch różnych przełącznikach oraz znacznie poprawi czas zbieżności sieci, gdyż wyeliminowane zostaną czasy niedostępności, charakterystyczne dla rekonfiguracji STP.
Dla połączenia przełączników w układ wirtualnego chassis wykorzystane będą porty 10Gb/s.
Wymagania:
Przełącznik szkieletowy dla sieci LOT (2 szt.)

- Przełącznik modularny czteroslotowy o wydajności przełączania co najmniej 640Gb/s dla warstwy 2 i co najmniej 480 Mpps dla warstwy 3
- Przełącznik musi być wyposażony co najmniej w 8 portów 10Gb/s oraz 12 portów 10/100/1000
- Każdy slot musi być podłączony do matrycy przełączającej/routującej szyną o przepustowości, co najmniej 160G full duplex. Przepustowość przełączania minimum 960 Mpps.
- Przełącznik musi mieć możliwość instalacji minimum 2 modułów zarządzających lub zarządzająco-przełączających w przypadku połączenia tych funkcji.
- Redundancja zasilania N+1. Zasilacze muszą pracować w trybie podziału obciążenia i zapewnić pełną wymaganą dla działania urządzenia moc w przypadku awarii jednego z zasilaczy
- Możliwość instalacji min. dwóch wersji oprogramowania systemowego
- Możliwość zapisania minimum 5 różnych wersji konfiguracji
- Pamięć minimum 1G oraz 1G dla pamięci Flash
- Pojemność tabeli MAC adresów min. 64 tys. wpisów
- Wsparcie dla min. 4090 sieci wirtualnych jednocześnie, wsparcie dla GVRP lub równoważne

- Możliwość klasyfikacji pakietów w L2 według:
  - Źródłowego adresu MAC
  - Docelowego adresu MAC
  - Źródłowego adresu IP
  - Docelowego adresu IP
  - UDP/TCP źródłowy port
  - UDP/TCP docelowy port
  - IP TOS
  - IP typ
  - IP Fragmentacja – klasyfikacja
- Obsługa Jumbo Frames (min. 9kB)
- Obsługa 8 kolejek priorytetów na każdym porcie
- Obsługa priorytetów zgodna z IEEE 802.1p
- Obsługa protokołów Spanning Tree – IEEE 802.1D, IEEE 802.1w, IEEE 802.1s
- Obsługa protokołu LLDP
- Obsługa Link Aggregation IEEE 802.3ad.
- Musi posiadać przynajmniej 200MB bufora pakietów dla każdego portu 10Gb/s
- Musi obsługiwać SNMPv1, SNMPv2c oraz SNMPv3
- Musi obsługiwać RMON (Statistics, History, Alarms, Events, Host, HostTopN, Matrix, Capture, Filter)
- Musi obsługiwać wiele mechanizmów kolejkowania (SPQ, WFQ, WRR, Hybrid)
- Musi obsługiwać kontrolę poziomu pasma wychodzącego i przychodzącego w każdym przepływie.
- Musi obsługiwać opcje Port/VLAN mirroring (jeden do jednego, jeden do wielu, wielu do wielu)
- Musi obsługiwać ograniczniki poziomu ruchu oparte o pasmo lub liczenie pakietów (pps), z progami pasma pomiędzy 8Kbps i 4Gbps.
- Musi obsługiwać technologię RADIUS Accounting
- Musi obsługiwać technologię TACACS+
- Musi mieć możliwość ograniczania liczby nowych lub ustanowionych przepływów, które mogą być zaprogramowane na indywidualnym porcie przełącznika by zwalczyć atak DoS
- Musi obsługiwać technologie IEEE 802.1X Port Based Network Access, uwierzytelnianie oparte o adres MAC oraz Port Based Web Authentication
- Musi obsługiwać dynamiczne i statyczne blokowanie portów oparte o adresy MAC

- Musi obsługiwać technologię VLAN-to-Policy mapping
- Musi obsługiwać LLDP oraz LLDP-MED.
- Musi zapewniać kompletne, niepodzielone(not sampled) dane NetFlow (v5/v9) lub równoważne, ale nie samplowane.
- Funkcjonalności warstwy 3
- Sprzętowa obsługa routingu IPv4 i IPv6
- Musi obsługiwać funkcje routingu, w tym: trasy statyczne, OSPF v1/v2, RIPv1/RIPv2, IPv4, routing Multicast (IGMP v1/v2/v3, PIM-SM), Policy Based Routing, Route Maps, VRRP.
- Musi posiadać mapę tras dla obsługi VRF (Virtual Routing and Forwarding).
- Obsługa IGMPv1/v2/v3
- Routing multicast PIM-SM
- Authentykacja MD5 dla protokołów routingu
- Zarządzanie
- Obsługa zewnętrznego systemu logowania zdarzeń SYSLOG, RMON(9 grup),
- Obsługa synchronizacji czasu w oparciu o zewnętrzny serwer SNTP lub NTP
- Obsługa SNMP v1/v2/v3
- Sprzętowa obsługa nie samplowanego NetFlow na każdym porcie bez straty wydajności urządzenia lub równoważne ale nie samplowane.
- Obsługa SSHv2 serwer i klient
- Obsługa Telnet
- Obsługa TFTP
- Obsługa TACACS+
- Obsługa RFC 3580
- Obsługa RADIUS (RFC 2865)
- Obsługa RADIUS Accounting (RFC 2866)
- Obsługa RADIUS EAP 802.1x

Przełącznik szkieletowy dla sieci SOL :

- Przełącznik 2U o wydajności przełączania co najmniej 320Gb/s dla warstwy 2 i co najmniej 240 Mpps dla warstwy 3
- Przełącznik musi być wyposażony co najmniej w 8 portów 10Gb/s oraz 12 portów 10/100/1000
- Każdy slot musi być podłączony do matrycy przełączającej/routującej szyną o

przepustowości, co najmniej 160G full duplex. Przepustowość przełączania minimum 960 Mpps.

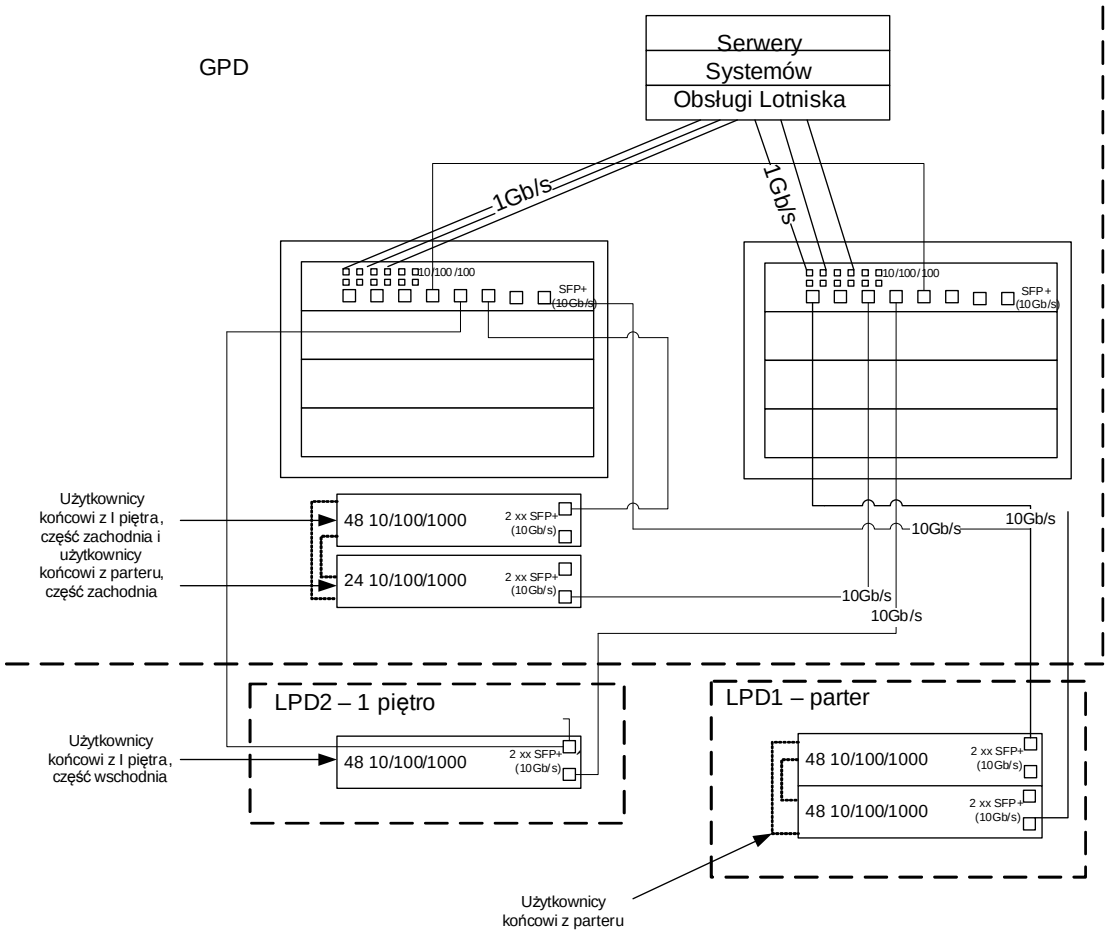
- Przełącznik musi mieć możliwość instalacji minimum 3 modułów zarządzających lub zarządzająco -przełączających w przypadku połączenia tych funkcji.
- Redundancja zasilania N+1. Zasilacze muszą pracować w trybie podziału obciążenia i zapewnić pełną wymaganą dla działania urządzenia moc w przypadku awarii jednego z zasilaczy
- Możliwość instalacji min. dwóch wersji oprogramowania systemowego
- Możliwość zapisania minimum 5 różnych wersji konfiguracji
- Pamięć minimum 1G oraz 1G dla pamięci Flash
- Pojemność tabeli MAC adresów min. 64 tys. wpisów
- Wsparcie dla min. 4090 sieci wirtualnych jednocześnie, wsparcie dla GVRP lub równoważne
- Możliwość klasyfikacji pakietów w L2 według:
    - Źródłowego adresu MAC
    - Docelowego adresu MAC
    - Źródłowego adresu IP
    - Docelowego adresu IP
    - UDP/TCP źródłowy port
    - UDP/TCP docelowy port
    - IP TOS
    - IP typ
    - IP Fragmentacja – klasyfikacja
- Obsługa Jumbo Frames (min. 9kB)
- Obsługa 8 kolejek priorytetów na każdym porcie
- Obsługa priorytetów zgodna z IEEE 802.1p
- Obsługa protokołów Spanning Tree – IEEE 802.1D, IEEE 802.1w, IEEE 802.1s
- Obsługa protokołu LLDP
- Obsługa Link Aggregation IEEE 802.3ad.
- Musi posiadać przynajmniej 200MB bufora pakietów dla każdego portu 10Gb/s
- Musi obsługiwać SNMPv1, SNMPv2c oraz SNMPv3
- Musi obsługiwać RMON (Statistics, History, Alarms, Events, Host, HostTopN, Matrix, Capture, Filter)
- Musi obsługiwać wiele mechanizmów kolejkowania (SPQ, WFQ, WRR, Hybrid)

- Musi obsługiwać kontrolę poziomu pasma wychodzącego i przychodzącego w każdym przepływie.
- Musi obsługiwać opcje Port/VLAN mirroring (jeden do jednego, jeden do wielu, wielu do wielu)
- Musi obsługiwać ograniczniki poziomu ruchu oparte o pasmo lub liczenie pakietów (pps), z progami pasma pomiędzy 8Kbps i 4Gbps.
- Musi obsługiwać technologię RADIUS Accounting
- Musi obsługiwać technologię TACACS+
- Musi mieć możliwość ograniczania liczby nowych lub ustanowionych przepływów, które mogą być zaprogramowane na indywidualnym porcie przełącznika by zwalczyć atak DoS
- Musi obsługiwać technologie IEEE 802.1X Port Based Network Access, uwierzytelnianie oparte o adres MAC oraz Port Based Web Authentication
- Musi obsługiwać dynamiczne i statyczne blokowanie portów oparte o adresy MAC
- Musi obsługiwać technologię VLAN-to-Policy mapping
- Musi obsługiwać LLDP oraz LLDP-MED.
- Musi zapewniać kompletne, niepodzielone(not sampled) dane NetFlow (v5/v9) lub równoważne, ale nie samplowane.
- Funkcjonalności warstwy 3
- Sprzętowa obsługa routingu IPv4 i IPv6
- Musi obsługiwać funkcje routingu, w tym: trasy statyczne, OSPF v1/v2, RIPv1/RIPv2, IPv4, routing Multicast (IGMP v1/v2/v3, PIM-SM), Policy Based Routing, Route Maps, VRRP.
- Musi posiadać mapę tras dla obsługi VRF (Virtual Routing and Forwarding).
- Obsługa IGMPv1/v2/v3
- Routing multicast PIM-SM
- Authentykacja MD5 dla protokołów routingu
- Zarządzanie
- Obsługa zewnętrznego systemu logowania zdarzeń SYSLOG, RMON(9 grup),
- Obsługa synchronizacji czasu w oparciu o zewnętrzny serwer SNTP lub NTP
- Obsługa SNMP v1/v2/v3
- Sprzętowa obsługa nie samplowanego NetFlow na każdym porcie bez straty wydajności urządzenia lub równoważne ale nie samplowane.
- Obsługa SSHv2 serwer i klient
- Obsługa Telnet

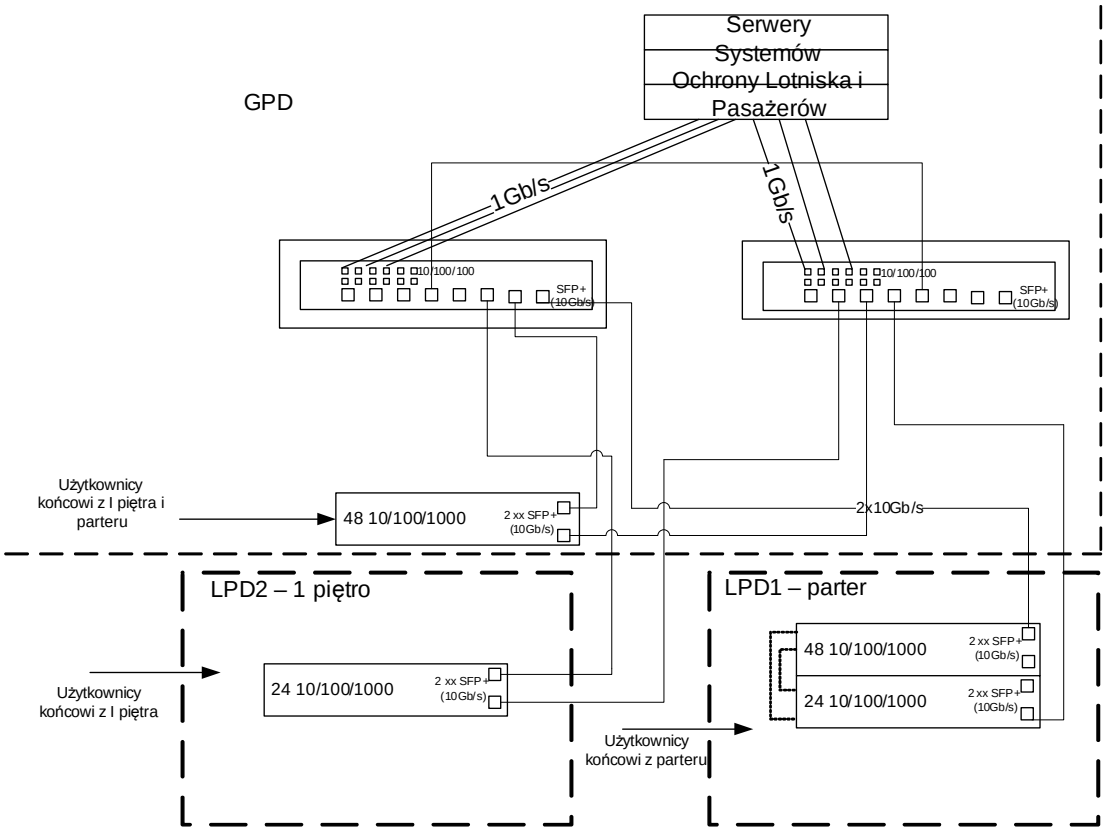
- Obsługa TFTP
- Obsługa TACACS+
- Obsługa RFC 3580
- Obsługa RADIUS (RFC 2865)
- Obsługa RADIUS Accounting (RFC 2866)
- Obsługa RADIUS EAP 802.1x

Rozmieszczenie i sposób połączeń przełączników

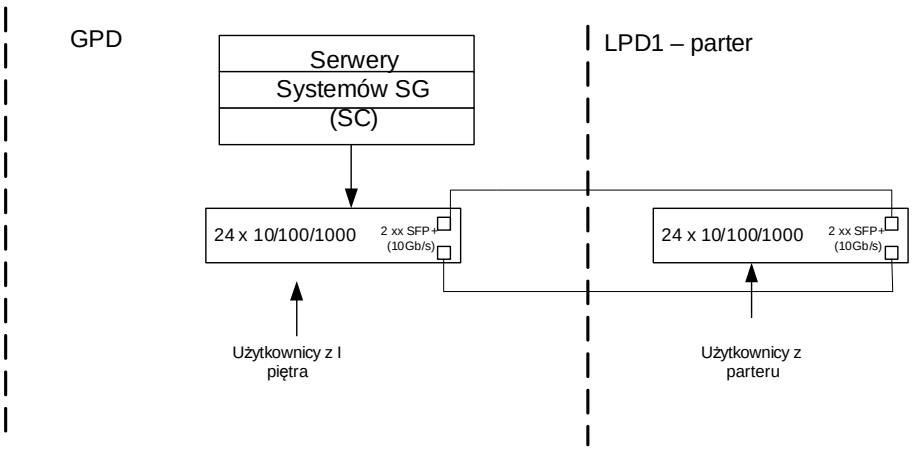
Poniżej przedstawiono rysunki obrazujące rozmieszczenie i sposób połączeń pomiędzy przełącznikami poszczególnych sieci.



Przełączniki sieci LOT



Przełączniki sieci SOL



Przełączniki sieci SG (przełączniki sieci SC tak samo)

Sieć bezprzewodowa WLAN

Do celów komunikacji bezprzewodowej projektuje się system sieci WLAN w oparciu o centralny kontroler i punkty dostępowe AP. Punkty dostępowe będą włączane do sieci przewodowej LOT.

Logicznie sieć bezprzewodowa powinna stanowić wydzieloną domenę bezpieczeństwa, a cały ruch kierowany przez Moduł dostępu do internetu i bezpiecznej komunikacji pomiędzy sieciami.

- System sieci bezprzewodowej musi integrować się bezproblemowo z dostarczaną infrastrukturą przewodową i być zarządzany przez ten sam system zarządzania siecią.
- Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości 802.11a/n (5 GHz) i 802.11b/g/n (2.4 GHz).
- Punkty dostępowe muszą obsługiwać technologię 802.11n i pracę w technice transmisji wieloantenowej MIMO 3x3 przy zasilaniu przez jedno źródło zgodne z 802.3af, bez wpływu na działanie kluczowych funkcji.
- Musi posiadać certyfikat 802.11n WiFi dla kompatybilności w sieciach WLAN.
- Punkty dostępowe muszą być zgodne z DFS2 (Dynamic Frequency Selection) by dopuścić dodatkowe kanały w paśmie 5 GHz.
- Punkty dostępowe muszą obsługiwać WDS (Wireless Distribution System) z możliwością tworzenia łączy typu backhaul na dowolnym łączu radiowym lub wykorzystania jednego łącza radiowego zarówno na potrzeby backhaul, jak i świadczenia usług klientom.
- Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g oraz 802.11n. Proszę opisać jak ta funkcjonalność jest realizowana.
- Punkt dostępowy musi obsługiwać instalację typu plug&play.
- System musi umożliwiać centralne wdrażanie konfiguracji i aktualizacji.
- Kontrolery muszą obsługiwać elastyczne opcje wdrożenia, obsługując zarówno scentralizowaną, jak i rozproszoną architekturę. Proszę o opisanie architektury kontrolera.
- Punkty dostępowe muszą jednocześnie obsługiwać ruch tunelowany i mostowany.
- Punkty dostępowe muszą obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń.
- Musi obsługiwać standardy uwierzytelniania i szyfrowania, w tym: WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x.
- Musi posiadać portal dostępowy Captive Portal zintegrowany z kontrolerem, który można dowolnie dostosowywać do potrzeb.
- Musi pozwalać nietechnicznym pracownikom na tworzenie tymczasowych kont gości i dystrybuowanie zezwoleń poprzez łatwy w użyciu graficzny interfejs użytkownika.
- Punkt dostępowy musi wspierać inteligentne szyfrowanie, tworzenie czarnych list, filtrowanie oraz QoS, niezależnie od kontrolera.

- Punkt dostępowy musi zapewniać rozproszone zarządzanie łącznością radiową RF Management (Radio Frequency), niezależne kontrolera - poza tylko wstępną konfiguracją. Po utracie połączenia z kontrolerem, punkt dostępowy musi być zdolny do zapewnienia ciągłości operacji związanych z szyfrowaniem, tworzeniem czarnych list, filtrowaniem, QoS oraz zarządzaniem łącznością radiową, zarówno dla swoich potrzeb, jak i lokalnie mostowanego ruchu.
- Punkty dostępowe muszą mieć możliwość wdrożenia w formie sensorów sieci – pracujących w pełnym lub niepełnym wymiarze czasu.
- Musi obsługiwać funkcje egzekwowania polityk i ograniczania przepustowości w punkcie dostępowym. Prosimy o opisanie tych możliwości.
- Zarządzanie łącznością radiową RF Management musi obsługiwać funkcje automatycznego wyboru kanału i automatycznej kontroli mocy emitowanego sygnału TPC (Transmit Power Control).
- W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie i bez interwencji użytkownika.
- Zarządzanie łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika.
- Punkty dostępowe sieci WLAN muszą mieć możliwość konfiguracji zapewniającej równoważenie obciążenia i sterowanie pasmem. Ta funkcja pozwala punktom dostępowym na równoważenie/sterowanie ruchem klientów pomiędzy obiema częstotliwościami na jednym punkcie dostępowym i/lub pomiędzy wieloma punktami dostępowymi w ramach domeny łączności radiowej.
- Punkty dostępowe muszą mieć możliwość wdrożenia w konfiguracji kratowej, tworzącej bezprzewodowe, wzajemne połączenia pomiędzy poszczególnymi punktami dostępowymi.
- Musi obsługiwać wiele typów kontrolerów dla różnych typów wdrożeń sieci.
- Kontrolery i punkty dostępowe muszą obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence.

- Punkty dostępowe muszą obsługiwać protokoły 802.11e, w tym WMM, TSPEC oraz U-APSD.
- Musi obsługiwać szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC).
- Musi obsługiwać do 16 SSID (8 na częstotliwość radiową).
- Musi obsługiwać RADIUS Authentication & Accounting.
- Kontrolery muszą obsługiwać różne mechanizmy przekazywania danych, w tym routing i mostowanie. Mechanizm przekazywania danych musi być skonfigurowany w podziale na wirtualne grupy sieciowe.
- Musi obsługiwać płynny roaming pomiędzy podsieciami IP.
- Musi obsługiwać płynny roaming pomiędzy wieloma kontrolerami.
- Musi obsługiwać przypisywanie polityk klientom, bez konieczności segmentacji przez dedykowane SSID.
- Musi oferować polityki oparte na rolach zapewniające bezpieczeństwo, kontrolę dostępu i priorytety QoS, aplikowane względem użytkownika i aplikacji,
- Musi obsługiwać ujednoliconą, opartą na rolach kontrolę dostępu do sieci przewodowej i bezprzewodowej. Prosimy opisać w jaki sposób jest to realizowane.
- Punkt dostępowy musi być zgodny z normami:
- R&TTE Directive 1999/5/EC
- EN 301 893
- EN 300 328
- 89/336/EEC EMC Directive
- EN 301 489 -1 & 17
- EN55011/CISPR 11 Class B, Group 1 ISM
- EN55022/CISPR 22 Class B
- EN55024/CISPR 24
- EN 300 386
- EN / UL 60601-1-2
- EN 50385
- Punkt dostępowy musi mieć możliwość zasilania poprzez skrętkę zgodnie ze standardem IEEE 802.3af

Rozmieszczenie punktów dostępowych należy zaplanować na podstawie pomiarów i projektu wykonawczego przygotowanego na etapie realizacji. Wstępnie planuje się.

Parter – 5 punktów dostępowych AP oraz 3 dedykowane sensory AP.
I Piętro – 5 punktów dostępowych AP oraz 3 dedykowane sensory AP.

Moduł dostępu do internetu i bezpiecznej komunikacji pomiędzy sieciami

~~Dostęp do internetu zostanie zabezpieczony przez parę urządzeń typu Next Generation Firewall~~, realizujące funkcje firewalli i IPS. Urządzenia te będą zabezpieczać zarówno komunikację z internetem jak i komunikację pomiędzy sieciami poszczególnych służb.
Zastosowany firewall oferuje szerokie możliwości ochrony sieci. Poniżej przedstawiono cech charakterystyczne rozwiązania:

- Technologia App-Id - filtrowanie ruchu sieciowego na podstawie zbioru reguł opartego na rzeczywistych aplikacjach (a nie samych portach)
- Kilkaset wbudowanych profili aplikacyjnych obejmujących takie protokoły i serwisy Web 2.0 jak n.p.: BitTorrent, lastfm, GaduGadu, GMail, Skype, Tor, WebEx.
- Obsługa HTTPS poprzez wbudowane proxy i wewnętrzny urząd certyfikatów
- Sieci VPN: IPsec, route-based VPN, 3DES, AES (128,192,256 bit); SHA-1, KD5
- Inspekcja danych: antywirus, filtr URL-i, IPS; filtracja plików
- Filtrowanie URL: minimum 76 kategorii, baza danych mimimum 20 mln adresów (lokalna), własna baza użytkownika,
- Integracja z NAC
- Praca w trybach L2, L3, Tap, Virtual Wire
- Wirtualne rutery, wirtualizacja i klastry HA
- Zarządzanie poprzez intuicyjny przeglądarkowy interfejs graficzny - funkcje drag-and-drop, itp.
- Rozbudowane raportowanie - wbudowane raporty w postaci tabelarycznej i graficznej, obsługa Syslog, SNMPv2,
- Netconnect SSL VPN: SSL/IPSec, autoryzacja LDAP, SecureID. Klient: Windows XP/Vista/7 (32 i 64 bit);
- Ruting: OSPF, RIP, BGP,
- Obsługa VLAN
- QoS: 8 klas ruchu, ustalanie priorytetów wg. polityki bezpieczeństwa (aplikacja, źródło, przeznaczenie, interfejs, tunel VPN, ...),
- Wieloprocesorowa architektura: procesory ogólnego przeznaczenia oraz procesor sieciowy dedykowane do zadań takich jak: zarządzanie, obsługa regul filtracji, NAT, QoS, szyfrowania SSL i IPsec

- Interfejsy: 12x Ethernet 10/100/1000 ,8x SFP (1Gbps)
- Integracja z systemem kontroli dostępu do sieci , pozwalająca na identyfikację ruchu ruchu należącego do poszczególnych użytkowników sieci i przypisanie indywidualnych reguł firewall na podstawie uwierzytelnienia w systemie kontroli dostępu do sieci.

Do analizy przyjęto PA3050. Można zastosować elementy rónoważne innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż przyjęte w projekcie.

Punkt dystrybucyjny	Szafa/sieć	Serwer/urządzenie	Opis	ilość	miejsce [U]*	moc (W)*	I max [A]*	ciepło tracone BTU/h*
GPD		PA3050	Firewall	2	1	250	1	683

*na jedno urządzenie

Można zastosować elementy rónoważne innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż przyjęte w projekcie.

Koncepcja bezpieczaństwa projektowanej sieci

Infrastruktura sieciowa posiadać będzie możliwości obsługi wielu grup użytkowników (multi-client). Dodatkowe usługi takie jak telefonia VoIP z priorytetyzacją ruchu (QoS) i dostęp do Internetu zostaną udostępnione dla każdej z tych grup. Poszczególni użytkownicy mogą być dołączani w każdym z punktów sieci. Poszczególne sieci będą być odizolowane w sposób logiczny od pozostałych sieci na terenie obiektu.

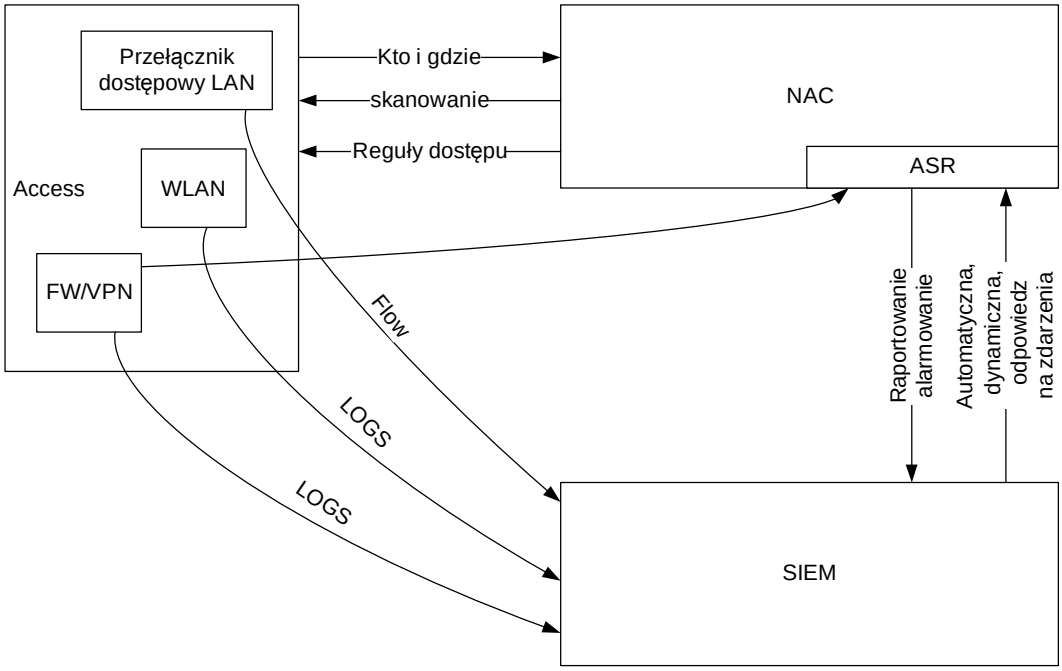
W momencie dołączania do sieci, następować będzie uwierzytelnienie użytkownika.

Przewidywane są trzy metody uwierzytelnienia:

- Przy zastosowaniu 802.1x
- Webbased
- Oparta na MAC adresach dla prostych urządzeń sieciowych jak np. drukarki nie obsługujące 802.1x

Wszystkie maszyny włączane do sieci będą być skanowane w celu uniknięcia dołączania maszyn zainfekowanych wirusami lub posiadających wersje systemów operacyjnych szczególnie narażonych na ataki hakerów (bez aktualnych poprawek).

System zarządzania będzie pozwalać na łatwe i pewne przydzielanie dozwolonych przez politykę bezpieczeństwa usług i aplikacji do poszczególnych sieci logicznych, grup użytkowników, adresów IP/MAC i fizycznych portów na przełączniku



Rysunek 3 Koncepcja bezpieczeństwa projektowanej sieci

Wdrażane rozwiązania pozwolą na integrację z nadrzędnym systemem Security Information and Event Management, który pozwoli na korelację informacji o zdarzeniach istotnych dla bezpieczeństwa, alarmowanie i raportowanie oraz automatyczną odpowiedź sieci w przypadku wykrycia zagrożeń.

Kontrola dostępu do sieci LAN

Zaprojektowano system kontroli dostępu do sieci Network Access Control (NAC) jako niezbędny element systemu bezpieczeństwa organizacji. Wdrożenie NAC musi zapewnić więcej niż jedynie prostą, jednorazową kontrolę dostępu, z elementami oceny stanu zabezpieczeń urządzeń końcowych . Zastosowane rozwiązanie Network Access Control musi być dynamiczne, trwałe i funkcjonować na bieżąco. Rozwiązania NAC muszą zapewniać szczegółowe polityki bezpieczeństwa, które mogą być egzekwowane w dowolnym czasie, i które znają treść komunikacji pomiędzy punktami końcowymi a infrastrukturą IT

System NAC będzie świadczyć dostęp do zasobów i usług sieciowych w oparciu o informacje takie jak uwierzytelniona tożsamość użytkownika lub urządzenia, położenie, czas oraz aktualny lub historyczny stan zabezpieczeń urządzenia. Na podstawie tych kryteriów przyznawane będą przywileje dostępu. Systemy niezgodne będą poddawane kwarantannie w celu korekcji swojego stanu zabezpieczeń lub bedą rejestrowane dla potrzeb późniejszej oceny. System stale monitoruje użytkowników i punkty końcowe by zapewnić pewność, że działają oni normalnie, zgodnie z przyjętymi zasadami użytkowania (politykami). Systemy niezgodne muszą być przenoszone do kwarantanny i muszą korygować stan swoich zabezpieczeń, co ma na celu ochronę sieci przed propagacją zagrożeń.

System kontroli dostępu do sieci musi zapewnić widoczność i kontrolę poszczególnych użytkowników oraz aplikacji pracujących w sieciach wykorzystujących rozwiązania różnych dostawców. Polityki systemu mają za zadanie przepuszczać lub odrzucać ruch sieciowy, nadawać mu priorytety, ograniczać w razie potrzeby jego szybkość, tagujować, przekierowywać i kontrolować go w oparciu o tożsamość użytkownika, czas, położenie, typ urządzania, itp. System musi obsługiwać kwarantannę opartą o port RFC3580 i VLAN dla różnych typów przełączników oraz silniejsze polityki izolacji dla przełączników wykorzystanych projekcie sieci portu lotniczego (tak aby zagrożone punkty końcowe znajdujące się w kwarantannie były wzajemnie izolowane od siebie i nie zostały wykorzystane do przeprowadzania ataków na sieć)..

System kontroli dostępu do sieci musi wspomagać korygowanie systemów końcowych niezgodnych ze zdefiniowanymi politykami bezpieczeństwa. Urządzenie NAC będzie zapewnia funkcje korygowania poprzez uruchomiony na nim Web Server.Ma on zadanie informować on użytkowników końcowych, gdy ich systemy zostały poddane kwarantannie w wyniku niezgodności z politykami bezpieczeństwa i pozwalać użytkownikom na bezpieczną naprawę swoich systemów bez pomocy działu IT.

System kontroli dostępu do sieci musi wykorzystywać te same, centralne bazy danych co wszystkie pozostałe aplikacje Zarządzania Siecią i będzie informować o wszystkich systemach chcących uzyskać dostęp do sieci, włączając w to wszystkie punkty końcowe. System NAC może wykorzystać zarówno technologie 802.1X jak i adres MAC dla potrzeb autoryzacji i uwierzytelniania systemów w sieci. Aplikacja musi umożliwiać dokładną prezentacje różnych systemów podłączających się do sieci oraz ich lokalizacje.

Serwer uwierzytelniający dostęp do sieci powinien zostać zainstalowany w postaci czterech oddzielnych instancji w postaci maszyn wirtualnych , po jednej dla każdej z sieci (LOT, SOL, SG,SC).

Rozwiązanie nadzorujące dostęp do sieci NAC, powinno charakteryzować się następującymi minimalnymi właściwościami:
Rozwiązanie musi łączyć ze sobą zdolność zabezpieczenia różnorodnych sieci w jedno spójne rozwiązanie realizując autentykację oraz ocenę/weryfikację dla systemów operacyjnych typu Microsoft, Linux, Solaris, AIX, MacOS, xBSD.
Rozwiązanie musi realizować autentykacje bazując na standardach, detekcje, ocenę, kwarantannę, rekultywację, autoryzację przy i po połączeniu maszyn końcowych.

- Musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych punktów końcowych i innych niechronionych systemów
- Musi elastycznie obsługiwać wiele metod uwierzytelniania wielu użytkowników i urządzeń różnych dostawców.
- Rozwiązanie musi wykorzystywać oparte na standardach mechanizmy uwierzytelniania dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania I autoryzacji podłączanych systemów końcowych.
- Rozwiązanie musi obsługiwać uwierzytelnianie RADIUS i LDAP.
- Musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, sesji wykorzystujących przeglądarkę internetową, oraz Kerberos) lub żądań RADIUS pochodzących z przełączników dostępowych.
- Musi współpracować z rozwiązaniem Microsoft NAP.
- Rozwiązanie musi obsługiwać lokalną autoryzację MAC.
- Musi przeprowadzać przed- i po-połączeniowe ocenianie stanu zabezpieczeń systemów końcowych.
- Powinien posiadać możliwość rozbudowy o opcje oceniania w oparciu o agentów lub sieć (skanowania sieci).
- Musi umożliwiać ciągłe mechanizmy analizowania zagrożeń, zapobiegania im i przechowywania ich.
- Musi mieć zdolność ciągłego przypisywania polityk określonemu użytkownikowi, adresowi MAC lub OUI adresu MAC, tak, aby użytkownik, urządzenie lub grupa urządzeń miały przydzielony ten sam zestaw zasobów sieci, niezależnie od swojej lokalizacji lub konfiguracji serwera RADIUS.
- Rozwiązanie musi zapewniać informacje o typie urządzeń działających w sieci oraz określonych potrzebach i zagrożeniach, które są z nimi związane.
- Musi zapewnić rozwiązanie oferujące jednolity, centralny obraz wszystkich niechronionych

elementów związanych z użytkownikami i urządzeniami, który pozwoli później zredukować złożoność procesu zarządzania.

- Musi dostarczyć rozwiązanie, które zapewni ciągłość działania organizacji poprzez oferowanie użytkownikom alternatywnych metod dostępu podczas procesu skanowania.
- Rozwiązanie musi umożliwiać przypisanie na stałe adresu MAC do określonego przełącznika lub portu przełącznika. Jeżeli system końcowy będzie próbował się uwierzytelnić na innym porcie lub przełączniku, zostanie odrzucony lub przypisana mu zostanie polityka w oparciu o akcje określoną podczas przypisywania mu portu MAC.
- Musi umożliwiać monitorowanie zdarzeń systemów końcowych i przedstawianie wyników o stanie zabezpieczeń systemu w oparciu o najbardziej aktualne skanowania przeprowadzane podczas oceniania.
- Musi posiadać możliwość szybkiego podglądu historycznych i ostatnich znanych stanów połączeń dla każdego systemu końcowego i uzyskiwać informacje o znalezionych podczas skanowania zagrożeniach bezpieczeństwa systemu końcowego.
- Musi zapewnić kompleksowe raportowanie zgodności w oparciu o aktualne i historyczne informacje.
- Musi obsługiwać powiadamianie poprzez syslog, pocztę elektroniczną oraz usługi webowe o zmianach stanu systemów końcowych, rejestracji gości oraz wynikach skanowania stanu zabezpieczeń systemów końcowych.
- Musi zapewniać rozwiązanie NAC typu inline oraz out-of-band, które może być zarządzane przez jedną centralną aplikację.
- Musi obsługiwać polityki umożliwiające przepuszczanie lub odrzucanie ruchu sieciowego, nadawanie mu priorytetów, ograniczanie jego szybkości, tagowanie, przekierowywanie i kontrolowanie go w oparciu o tożsamość użytkownika, czas i położenie, typ urządzenia i inne zmienne środowiskowe.
- Musi posiadać funkcję IP-to-ID Mapping, która łączy razem nazwę użytkownika, adres IP, adres MAC oraz port fizyczny każdego punktu końcowego. Ta funkcjonalność jest kluczowa dla potrzeb audytów bezpieczeństwa i analiz dochodzeniowych
- Musi posiadać łatwy w obsłudze panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć systemów końcowych.
- Musi posiadać funkcję portalu rejestracyjnego dla kontroli dostępu gości, by zapewnić bezpieczne korzystanie z sieci przez gości, bez udziału pracowników działu IT. Musi także oferować zaawansowane możliwości sponsorowania dostępu takie, jak sponsorowanie

email oraz prosty portal dla sponsorów służący do zatwierdzania rejestracji gości. Może być również dostarczone, jako oddzielne rozwiązanie z minimalną licencją dla 100 gości i możliwą rozbudową do 300 gości.

- Powinien posiadać opcje urządzenia wirtualnego pozwalając na wykorzystanie istniejącego sprzętu i umożliwiać autoryzacje minimum 300 sesji/użytkowników w tym samym czasie.
- Nie dopuszcza się stosowania pakietów darmowych lub wersji testowych (ang. trial) oprogramowania komercyjnego ze względu na brak odpowiedniego wsparcia serwisowego dla takich produktów.

Integracja kontroli dostępu do sieci z modułem firewall

Rozwiązanie bezpieczeństwa będzie w stanie zidentyfikować użytkownika związanego z adresem IP i konkretną używaną aplikacją, nawet jeśli jest to jedna z wszechobecnych aplikacji internetowych, przechodzących przez port 80/443. System skojarzy adres IP z aktywnym użytkownikiem, gdyż system Network Access Control (NAC) i przełączniki dostępowe będą wiedzieć, jakich aplikacji używa system końcowy. Jest to rozwiązanie o wiele bardziej efektywne od opartego o integrację Firewalla z systemem LDAP / Active Directory (AD) . W takim przypadku skojarzenie adresu IP do mapowania użytkownika często informacją nieaktualną lub wprowadzają w błąd, ponieważ LDAP / AD nie wie, kiedy użytkownik rozłącza się z siecią..
Wdrażane rozwiązanie bazujące na integracji z systemem NAC dodatkowo pozwala określić gdzie użytkownik łączy się z siecią, w sposób przewodowy lub bezprzewodowy, ze strefy bezpiecznej czy publicznej. Dzięki integracji z systemem NAC uzyskuje się również mapowanie użytkownika dla dostępu gościnnego, co nie byłoby możliwe przy wykorzystaniu do tego celu LDAP / AD
Wymagana jest funkcjonalność “User to IP Mapping at Point of Connection “
System musi realizować mapowanie użytkowników do adresów IP w punkcie podłączenia użytkownika. System kontroli dostępu do sieci musi udostępniać firewallowi precyzyjne i dynamiczne mapowanie adresu IP do nazwy użytkownika.
System kontroli dostępu do sieci musi rozpoznać gdy użytkownik podłącza się do sieci przewodowej lub bezprzewodowej, uwierzytelnić go i przesyłać adres IP address / username / lokalizację/przydzieloną do firewalla politykę . Dla lokalnie uwierzytelnionych gości portal gościnny systemu kontroli dostępu do sieci przesyła właściwe mapowanie Guest Access username do IP.
Integracja firewalla z systemem zarządzania siecią i przełącznikami obsługującymi polityki bezpieczeństwa musi pozawalać na automatyczne reagowanie i dynamiczne przydzielanie polityk bezpieczeństwa w punkcie podłączenia do sieci w tym zarówno przewodowej jak i

bezprzewodowej. W sytuacji gdy firewall wykryje zagrożenie lub wrogie pakiety przesyłane z interfejsu użytkownika wewnętrznego informuje o tym zdarzeniu system kontroli dostępu do sieci i przekazuje adres IP użytkownika. System kontroli dostępu do sieci zlokalizuje wtedy port dostępowy użytkownika skojarzonego z danym adresem, zablokuje ruch przydzielając politykę kwarantanny i , wpisze nazwę użytkownika na czarną listę. Jeśli użytkownik będzie próbował podłączyć się do innego portu lub przez sieć bezprzewodową, ciągle będzie w kwarantannie.

System zarządzania siecią

System zarządzania siecią musi składać się z następujących modułów: moduł zarządzania urządzeniami, moduł inwentaryzacyjny moduł zarządzania politykami bezpieczeństwa, moduł kontroli dostępu do sieci oraz moduł automatyzacji bezpieczeństwa.

Rozwiązanie musi zapewnić widoczność i szczegółową kontrolę środowiska sieciowego.

Moduł zarządzania urządzeniami musi stanowić zestaw narzędzi pozwalających na centralne monitorowanie stanu urządzeń, definiowanie konfiguracji sieci i automatyzacje zadań związanych z rozwiązywaniem problemów. Moduł musi zapewniać centralny punkt podglądu i kontroli do zarządzania elementami infrastruktury oraz kompleksową widoczność kontrolerów sieci bezprzewodowych, punktów dostępowych i ruchomych klientów. Rozwiązanie musi być oparte na standardach i może zarządzać całą infrastrukturą sieci zgodną z SNMPv1, SNMPv2 lub SNMPv3. Dla zwiększenia funkcjonalności mogą być zainstalowanie specjalne MIB innych dostawców.

Moduł Inwentaryzacyjny musi służyć zarządzania wieloma urządzeniami, oraz zapewniać oprogramowanie firmware na poziomie systemowym oraz informacje konfiguracyjne i katalogujące sprzęt. Musipozwalać administratorom sieci na tworzenie spisów i zarządzanie zmianami komponentów i konfiguracji sieci. Moduł musi zapewnić scentralizowane zarządzanie oprogramowaniem i kopie zapasowe konfiguracji kontrolerów sieci bezprzewodowych. Moduł musi utrzymywać zorganizowaną, centralną bazę danych do gromadzenia danych i tworzenia raportów z historycznymi informacjami.

Moduł zarządzania politykami bezpieczeństwa musi automatyzować definiowanie i egzekwowanie w całej sieci polityk dla użytkowników, aplikacji, protokołów, sieci VLAN i portów. Wyeliminuje to konieczność konfigurowania polityk na każdym urządzeniu oddzielnie poprzez złożone komendy CLI. Polityki definiowane musza być przy pomocy graficznego interfejsu użytkownika aplikacji – jednokrotnie niezależnie od liczby zmian, aktualizacji, itp. – i następnie automatycznie egzekwowane na p urządzeniach sieciowych.

Moduł automatyzacji bezpieczeństwa musi bezpośrednio i automatycznie wykorzystywać informacje o zagrożeniach w celu ochrony sieci, w celu zautomatyzowania reakcji na incydenty bezpieczeństwa, korygując zagrożenia w czasie rzeczywistym. Moduł musi realizować oparte na

politykach reguły, a w momencie wywołania mapować adresy IP na porty i podejmować przypisane działania. Zakres możliwych działań w odpowiedzi na wywołanie musi być szeroki i konfigurowalny, obejmując m. in.: poddawanie kwarantannie użytkownika, wyłączanie portu przełącznika lub ograniczanie prędkości ruchu sieciowego. Podejmowanie działania nie może zakłócać pracy innych użytkowników.

Moduł kontroli dostępu do sieci musi zapewnić bezpieczne, oparte o polityki zarządzanie NAC. System zarządzania powinien być aplikacją dostarczoną dla zarządzania wszystkimi urządzeniami sieciowymi, system ten musi zapewnić:

- System musi umożliwiać zarządzanie do 50 urządzeń oraz umożliwiać rozbudowę, do co najmniej 250 urządzeń
- Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji.
- Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci.
- Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (OID).
- Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci po przez: MAC, IP, Maska, Adres Multicast, User Name
- Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz na dowolną zmianę terminu ich wykonania.
- Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB z reprezentacji opartej na drzewie, zawierające kompilator dla nowych MIB, w tym również dla tych pochodzących od różnych dostawców.
- Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN po przez GVRP lub równoważne.
- Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II.

Musi posiadać wbudowaną funkcjonalność serwera RADIUS lub należy dostarczyć komercyjny serwer RADIUS

- Musi zapewniać kompleksową obsługę do 300 użytkowników
- Musi umożliwiać dalsza rozbudowę do co najmniej 600 użytkowników.
- Nie dopuszcza się stosowania pakietów darmowych lub wersji testowych (ang. trial)

oprogramowania komercyjnego ze względu na brak odpowiedniego wsparcia serwisowego dla takich produktów.

Musi posiadać funkcjonalność serwera AAA i spełniać poniższe kryteria:

- System zarządzania dostępem do urządzeń oraz identyfikacji u uwierzytelniania użytkowników
- Musi obejmować oprogramowanie - dostarczane przez producenta dla uwierzytelnienia, autoryzacji oraz billingu (ang. accounting) użytkowników. Nie dopuszcza się stosowania pakietów darmowych lub wersji testowych (ang. trial) oprogramowania komercyjnego ze względu na brak odpowiedniego wsparcia serwisowego dla takich produktów.
- Musi komunikować się z urządzeniami sieciowymi z wykorzystaniem protokołów RADIUS lub TACACS, TACACS+
- Musi umożliwiać współpracę z routerami, przełącznikami sieciowymi, urządzeniami z funkcjonalnością firewall/IPS, w szczególności tymi opisanymi w innych punktach.
- Musi umożliwiać autoryzację użytkowników z wykorzystaniem protokołu 802.1x.
- Musi wpierać następujące protokoły uwierzytelniające: PAP, CHAP, MS-CHAP, EAP-TLS,
- Musi umożliwiać autoryzację użytkowników w oparciu o hasła stałe, jednorazowe (przy współpracy z odpowiednim serwerem) oraz z wykorzystaniem infrastruktury klucza publicznego PKI.
- Musi zapewniać szereg elastycznych mechanizmów kreowania polityki dostępu:
- Przypisanie użytkowników do VLAN na podstawie uwierzytelnienia i autoryzacji,
- Przypisanie listy kontroli dostępu per użytkownik,
- Musi zapewniać mechanizmy kontroli dostępu do systemu przez administratorów:

e) Ograniczenia działań dla wskazanych kont administratorów,

- Musi mieć możliwość ograniczenia adresów IP, z których można uzyskać dostęp do urządzenia.
- Musi wspierać protokół LDAP (ang. Lightweight Directory Access Protocol), Active Directory dla współpracy z systemami zewnętrznymi.
- Musi pracować w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci.
- Musi posiadać narzędzia replikacji z systemami redundantnymi.
- Licencja na minimum 50 użytkowników i urządzeń końcowych z możliwością rozbudowy do 250 użytkowników i urządzeń końcowych.
- Może być dostarczony, jako oddzielna aplikacja przy założeniu pełnej integracji z

pozostałymi aplikacjami opisanymi w specyfikacji.

Musi posiadać funkcjonalność kreowania i przypisywania uprawnień dla użytkowników, aplikacji, protokołów, portów i VLAN'ów w całym obszarze systemu i spełniać poniższe kryteria:

- Musi mieć możliwość definiowania uprawnień ograniczających poziom pasma, ograniczających liczbę nowych połączeń sieciowych, ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3, nadających tagi pakietom, izolujących/poddających kwarantannie poszczególne adresy IP, MAC, porty lub VLANy, uruchamiających wcześniej zdefiniowane działania.
- Musi posiadać możliwość wdrażania uprawnień w całej sieci tzn na przełącznikach, routerach, firewallach.
- Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika, niezależnie od miejsca jego logowania do sieci.
- Musi zapewniać łatwość wdrożenia i administracji uprawnień oraz rozwiązywania związanych z nimi problemów.
- Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).
- Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania.
- Musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC.
- Nie dopuszcza się stosowania pakietów darmowych lub wersji testowych (ang. trial) oprogramowania komercyjnego ze względu na brak odpowiedniego wsparcia serwisowego dla takich produktów.

Musi posiadać funkcjonalność zarządzania i inwentaryzacji sprzętu spełniając poniższe kryteria:

- Musi dostarczyć szczegółowy wykaz produktów zorganizowany według typu urządzenia.
- Musi umożliwiać śledzenie atrybutów urządzeń, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięci.
- Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania firmware, wielkość pliku.
- Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu.
- Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu urządzenia.
- Musi zapewniać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania spisem urządzeń.
- Musi umożliwiać generowanie wartościowych, szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych.

- Musi posiadać możliwość pobierania oprogramowania frimware do jednego urządzenia lub do wielu urządzeń jednocześnie.
- Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń.
- Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej ilości urządzeń.
- Nie dopuszcza się stosowania pakietów darmowych lub wersji testowych (ang. trial) oprogramowania komercyjnego ze względu na brak odpowiedniego wsparcia serwisowego dla takich produktów.

Musi posiadać funkcjonalność podejmowania dynamicznych zmian uprawnień dla użytkownika i portu na podstawie uzyskanej informacji z urządzeń bezpieczeństwa spełniając poniższe kryteria:

- Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania.
- Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku.
- Musi umożliwiać podejmowanie działań w oparciu o wcześniej określone schematy bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS/IPS oraz SIEM o podjętych działaniach poprzez komunikat SNMPv3 Trap (Inform).
- Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS/IPS i SIEM.
- Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci.
- Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia.
- Musi zapewniać dziennik zdarzeń i raportowanie.
- Musi nadawać rolę kwarantanny użytkownikowi podłączonemu do portu.
- Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji.
- Musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci.
- Może być dostarczone w formie zewnętrznego systemu np. SIEM
- Nie dopuszcza się stosowania pakietów darmowych lub wersji testowych (ang. trial) oprogramowania komercyjnego ze względu na brak odpowiedniego wsparcia serwisowego dla takich produktów.

Do celów instalacji systemu zarządzania siecią należy przewidzieć serwer wirtualizacyjny o następujących parametrach:

Jako platformę dla serwera uwierzytelniającego należy przewidzieć serwer o następujących parametrach: 5 fizycznych interfejsów sieciowych, pozostałe parametry zgodnie z wymaganiami aplikacji.

Moduł monitoringu systemu komunikacyjnego

Praca systemu komunikacyjnego będzie monitorowana przez centralny system monitorowania awarii – fault management o następujących parametrach:

- Monitorowanie awarii Softswitcha SIP
- Monitorowanie awarii urządzeń sieciowych
- Automatyczne rozpoznawanie elementów sieciowych
- Graficzny wielopoziomowy widok całej sieci
- Widok warstwy 2/3 sieci IP
- Diagnoza problemów w sieci
- Klient web pozwalający na dostęp do informacji o incydentach.
- Status sieci i systemów
- Planowane raporty zdarzeń i parametrów systemu

System zarządzania telefonami VoIP

Wraz z systemem dostarczone zostanie oprogramowanie umożliwiające zintegrowane zarządzanie urządzeniami IP (telefony IP). Oprogramowanie udostępniać będzie takie funkcje jak centralne zarządzanie wersjami oprogramowania telefonów i ich upgradowanie, zarządzanie konfiguracją, inventory management, zarządzanie bezpieczeństwem i usługi dla użytkowników końcowych takie jak Plug&Play oraz Mobility. Funkcja Plug&Play zapewnia automatyczną transmisję wszystkich paramatrów wymaganych przez urządzenie w momencie pierwszego podłączenia do sieci. Funkcja Mobility pozwala na zachowanie wszystkich ustawień osobistych użytkownika (jak układ klawiszy, książka telefoniczna, listy połączeń, tony dzwonka, wygaszacz ekranu) i udostępnienie ich w momencie, gdy użytkownik loguje się do dowolnego telefonu.

Oprogramowanie zapewni dynamiczną konfigurację telefonu IP w zależności od lokalizacji telefonu w sieci IP.

W systemie zarządzania w tej samej tabeli dostępne będą pola z następującymi danymi:

Numer telefonu- Adres IP telefonu – MAC adres telefonu - Nazwa przełącznika do którego podłączony jest telefon – Adres IP przełącznika – Numer portu na przełączniku – lokalizacja (budynek)- lokalizacja (pokój) – numer gniazdka – wersja oprogramowania telefonu

Funkcja	Opis
Automatyczna Inwentaryzacja	Automatyczna inwentaryzacja zapewnia informację o tym jaki telefon IP został włączony do sieci, jaka jest jego konfiguracja oraz gdzie jest zlokalizowany. Funkcja pozwala na kontrolę wszystkich zmian i przeniesień w ramach sieci.
Automatyczne dopasowanie	System zarządzania może wykorzystać informacje dotyczące danego telefonu do automatycznej rekonfiguracji w zależności od jednego z następujących parametrów: lokalizacja/wersja/model.
Monitoring telefonów IP	Przekazywanie informacji na temat wersji oprogramowania do nadrzędnego systemu zarządzania siecią w celu skierowania telefonów o nieaktualnej wersji oprogramowania do kwarantanny
Automatyczna informacja i powiadamianie o błędach	Informacja do użytkownika telefonu o błędzie uwierzytelnienia lub negatywnej weryfikacji zgodności z polityką bezpieczeństwa
Usługa lokalizacji fizycznej	Informacja dla administratora na którym porcie przełącznika został podłączony dany telefon.
Automatyczna autoryzacja	Dynamiczne przydzielenie odpowiedniego VLAN'u w raz z poziomem QoS i ustawieniami bezpieczeństwa
Ciągły monitoring telefonów IP	Informacja dla użytkownika telefonu o przeniesieniu telefonu do kwarantanny na skutek wykrycia ataku przez systemy detekcji intruzów (IDP)

Platforma wirtualizacyjna dla systemów zarządzania siecią

Systemy zarządzania siecią zostaną zaimplementowane w postaci maszyn wirtualnych w środowisku VMware. Wirtualizator zostanie zainstalowany na platformie hardwareowej serwera IBM Express x3650 M4 lub równoważnym.

Platforma wirtualizacyjna systemu telekomunikacyjnego

System telekomunikacyjny zostanie zaimplementowany w posaci maszyn wirtualnych wirtualnych w środowisku VMware. Wirtualizator zostanie zainstalowany na platformie hardwareowej serwera. Do analizy przyjęto IBM Express x3650 M4 lub równoważy.

Punkt dystrybucyjny	Szafa/sieć	Serwer/urządzenie	Opis	ilość	miejsce [U]*	moc (W)*	I max [A]*	ciepło tracone BTU/h*
GPD		x3650 M4	Platforma wirtualizacyjna dla systemów zarządzania siecią	1	2	2*550	3,3	Min conf: 525 Btu/hr Max conf: 3480
	LOT	x3650 M4	Platforma wirtualizacyjna dla centrali telefonicznej VoIP - serwera zunifikowanej komunikacji i aplikacji komunikacyjnych	1	2	2*550	3,3	Min conf: 525 Btu/hr Max conf: 3480

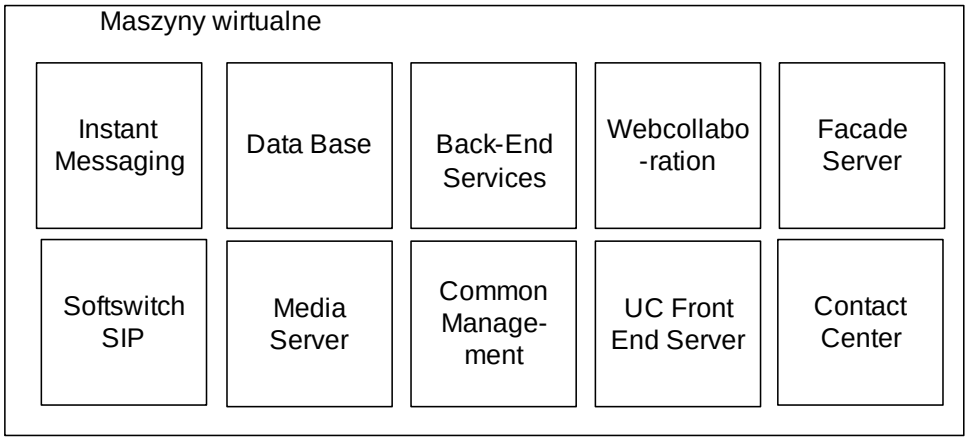
System monitorowania bezpieczeństwa sieci (SIEM) zostanie zainstalowany w postaci oddzielnego urządzenia. Do analizy przyjęto DSIMBA7-GB. Można zastosować inne równowazne rozwiązanie.

Punkt dystrybucyjny	Szafa/sieć	Serwer/urządzenie	Opis	ilość	miejsce [U]*	moc (W)*	I max [A]*	ciepło tracone BTU/h*
		DSIMBA7-GB	All-in-One Security Information and Event Management	1	1	2x502	brak danych	brak danych

System zunifikowanej komunikacji

Założenia dla systemu telekomunikacyjnego

Przedmiotem opracowania są wymagania dla systemu komunikacji głosowej i wideo dla potrzeb nowobudowanego terminala pasażerskiego. Do analizy, na potrzeby projektu przywołano konkretny system: mozna użyć rozwiązania równoważnego. Celem projektowanej instalacji jest zapewnienie nowoczesnych i efektywnych narzędzi komunikacyjnych dla pracowników poszczególnych służb portu lotniczego. Wszystkie urządzenia obsługujące komunikację podłączone zostaną do sieci służb administracyjnych, co uprości zarządzanie tym systemem, oraz pozwoli na ograniczenie ilości wykorzystanych przełączników pozwalających na zasilanie urządzeń końcowych w standardzie PoE poprzez zastosowanie ich tylko w tej sieci.



Rysunek - aplikacje komunikacyjne

Projektowany system zunifikowanej komunikacji, oparty będzie na serwerze typu softswitch, odpowiadającym za realizację połączeń głosowych i wideo opartych na protokole SIP. System uzupełniać będą serwery aplikacyjne, realizujące funkcjonalności media serwera, serwera zarządzającego, serwera zunifikowanego powiadamiania (poczta głosowa i faksowa, fax to mail, voice mailbox to mail itp), serwera zunifikowanej komunikacji. Ze względu na niewielką skalę systemu i ograniczone miejsce w szafach serwerowych , serwery aplikacyjne zostaną zrealizowane jako maszyny wirtualne zainstalowane w środowisku VMware.

Ze względu na fakt że pomimo rozwoju innych kanałów komunikacyjnych podstawową usługą komunikacyjną pozostaje komunikacja gosowa, istotne jest aby system dostarczający usługi zunifikowanej komunikacji posiadał silne wsparcie dla usług związanych z komunikacją głosową. Projektowany system zunifikowanej komunikacji to zestaw aplikacji umożliwiających: usługę jednego numeru (ONS), zawansowane usługi konferencji głosowych i multimedialnych,

zarządzanie dostępnością komunikacji (Presence) zależne od osób, czasu i formy komunikacji, tworzenie konferencji ze współdzieleniem dokumentów, agregację obsługi wielu form komunikacji jak mail, faks, SMS, wiadomości głosowe w jednym środowisku takim jak MS Outlook lub Lotus. „Ucyfrowienie" form komunikacji umożliwia prostą integrację z innymi strategicznymi systemami istniejącymi w firmie takimi jak elektroniczny obieg dokumentów, bazy wiedzy itp.
Do analizy, na potrzeby projektu przywołano konkretny system: mozna użyć rozwiązania równoważnego.

- Kluczowe elementy systemu tj: oprogramowanie Softswitch, oprogramowanie SBC, oprogramowanie Unified Communications, oprogramowanie telefonu programowego na PC obsługującego komunikację Wideo, oprogramowanie zaawansowanej usługi FMC i rozwiązanie bramy ISDN PRI będą pochodziły od jednego dostawcy.
- Kluczowe elementy systemu tj: oprogramowanie Softswitch, oprogramowanie SBC, oprogramowanie Unified Communications, uprawnienia użytkowników podstawowej i zaawansowanej usługi FMC, konfiguracja zaawansowanej usługi FMC i rozwiązanie bramy ISDN PRI będą posiadały wspólny system zarządzania. System ten zostanie dostarczony w ramach realizacji projektu.
- W celu zapewnienia komunikacji z różnymi centralami sąsiedzkimi oraz sieciami operatorów dostawca musi posiadać w ofercie moduły bram: ISDN 30B+D, ISDN 2B+D oraz FXO/FXS, które umożliwiają konwersję sygnału głosowego z postaci IP na TDM i odwrotnie.
- Powyższe moduły muszą pochodzić od producenta systemu i być objęte wspólnym zarządzaniem.
- W ramach wdrożenia Wykonawca przeprowadzi testy poprawności działania poszczególnych komponentów Systemu i przedstawi z nich raport.

Softswitch SIP

Do analizy, na potrzeby projektu przywołano konkretny system: mozna użyć rozwiązania równoważnego.

- System do realizacji usług głosowych w sieci IP musi opierać się na architekturze Softswitch i protokole SIP RFC3261 i działać wyłącznie w oparciu o komutację pakietów w sieci IP.
- System musi charakteryzować się otwartą architekturą, musi umożliwiać przyłączanie terminali różnych dostawców w oparciu o protokół SIP.

- System musi pozwalać na korzystanie z łączy SIP trunk, łącza SIP trunk i kanały głosowe w SIP trunk nie mogą być ograniczane licencjami (dodawanie kanałów głosowych w SIP trunk nie może wymagać wykupienia dodatkowych licencji).
- Podłączanie terminali obcych dostawców nie może wymagać wykupienia dodatkowych licencji lub dodatkowej liczby licencji innych niż dla telefonów dostawcy systemu, jeśli licencje takie są wymagane, należy doliczyć je w cenie do pełnej pojemności systemu.
- Pojedyncza licencja musi umożliwiać zarejestrowanie minimum 5 urządzeń o tym samym numerze.
- Nie dopuszcza się stosowania wersji testowych (ang. trial)
- System musi posiadać wbudowaną funkcjonalność firewall pozwalającą na blokowanie ruchu na podstawie parametrów warstw 2, 3, 4 modelu ISO/OSI.
- System musi dostarczać następujące funkcje dla użytkowników końcowych:
    - Prezentacja numeru abonenta dzwoniącego (CLIP) oraz blokada prezentacji numeru abonenta dzwoniącego (CLIR).
    - Interkom jednostronny - system musi realizować funkcję jednokierunkowego połączenia interkomowego. Uprawniony użytkownik aparatu systemowego (Abonent A) może wybrać kod dostępu do funkcji a następnie odbiorcę wyposażonego w aparat systemowy (Abonent B). Powoduje to zestawienie jednostronnego kanału komunikacji głosowej od abonenta A do abonenta B. Po użyciu funkcji głośnik w aparacie odbiorcy zostanie automatycznie włączony, a po rozłączeniu się abonenta A połączenie zostanie zakończone.
    - Interkom dwukierunkowy - system musi realizować funkcję dwukierunkowego połączenia interkomowego. Uprawniony użytkownik aparatu systemowego (Abonent A) może wybrać kod dostępu do funkcji a następnie odbiorcę wyposażonego w aparat systemowy (Abonent B). Powoduje to zestawienie dwukierunkowego kanału komunikacji głosowej pomiędzy abonentami A i B. Po użyciu funkcji głośniki i mikrofony w obu aparatach zostaną automatycznie włączone.
    - Prezentacja numeru abonenta, z którym jest zestawione połączenie (COLP) oraz blokada prezentacji numeru abonenta, z którym jest zestawione połączenie (COLR).
    - Prezentacja nazwy abonenta dzwoniącego (CNIP) oraz blokada nazwy abonenta dzwoniącego (CNIR).

- Prezentacja nazwy abonenta, z którym jest zestawione połączenie (CNIP) oraz blokada prezentacji nazwy abonenta (CNIR), z którym jest zestawione połączenie.
- Wizualna sygnalizacja rozmowy przychodzącej dla aparatów systemowych.
- Funkcjonalność „nie przeszkadzać” DND w oparciu o serwer z możliwością konfiguracji zachowania dla abonenta A: zastosowania przekierowania warunkowego lub odrzucenia połączenia z komunikatem o niedostępności.
- Obsługa połączeń oczekujących w sytuacji pracy normalnej i dla oddziałów wyposażonych w funkcje przetrwania również w czasie awarii WAN.
- Obsługa klawiszy szybkiego wybierania numerów.
- Transferowanie połączeń.
- Callback – oddzwonienie.
- Automatyczne wybieranie najlepszej drogi (z uwzględnieniem wag łączy).
- Narzędzia dynamicznego uaktualniania oprogramowania systemowego telefonów.
- Możliwość generowania raportów połączeń (Call Detail Reports) z aplikacji taryfikacyjnej.
- Funkcjonalność sekretarsko-dyrektorska.
- Możliwość realizacji usługi wideotelefonii z wykorzystaniem kamery i aplikacji instalowanej na stacji roboczej.
- Możliwość realizacji usługi wideotelefonii z wykorzystaniem aparatu systemowego doposażonego w kamerę USB.
- Możliwość realizacji usługi wideotelefonii z wykorzystaniem dedykowanego zestawu wideokonferencyjnego.
- Współpraca z aparatami telefonicznymi wspierającymi certyfikaty x509v3.
- Zabezpieczenie protokołów sygnalizacyjnych protokołem IPsec lub TLS.
- Zestawianie połączeń szyfrowanych na trasie od telefonu IP do telefonu IP protokołem SRTP.
- Mechanizm Call Admission Control, uwzględniający minimum połączenia głosowe, faksowe i wideo.

- Musi posiadać kompatybilne rozwiązanie poczty głosowej, możliwe do zintegrowania z systemami poczty elektronicznej, zarządzane przez przeglądarkę WWW.
- Zapewni współpracę z bramami głosowymi.
- Zapewni współpracę z SIP Proxy Server.
- Zapewni współpracę z urządzeniami klienckimi (telefony IP, oprogramowanie dla stacji roboczych) z wykorzystaniem protokołu SIP.
- Musi obsługiwać połączenia oczekujące.
- Musi obsługiwać wstrzymanie połączenia – Hold.
- Musi obsługiwać przejęcie połączenia.
- Musi obsługiwać linie wirtualne.
- Musi obsługiwać dynamiczne licencje użytkowników. Tzn umożliwiać już w wersji dostarczonej wygenerowanie abonentów do pełnej żądanej rozbudowy sytemu. Zakupione licencje dynamiczne muszą umożliwiać rejestrację wskazanej liczby abonentów SIP.
- System musi obsługiwać Interfejs One Number Service CSTA. Możliwość zarządzania wybieraniem i funkcjami abonenta za pomocą aplikacji komputerowej z interfejsem CSTA w taki sposób aby niezależnie od tego na jakim fizycznym urządzeniu wykonywana lub odbierana jest rozmowa abonent B widział stały numer abonenta A zdefiniowany w usłudze ONS.
- Prywatna lista szybkiego wybierania definiowana przez użytkownika. Możliwość zdefiniowania listy do 25 numerów.
- Prywatna lista szybkiego wybierania współdzielenie. Możliwość zdefiniowania listy jako współdzielonej z innymi użytkownikami systemu.
- Systemowa lista szybkiego wybierania definiowana przez administratora. Możliwość zdefiniowania 10 list do 1000 numerów i przypisania min 2 list każdemu użytkownikowi.
- Secure Shell w wersji 2 dla Interfejsu Zarządzania.
- Wsparcie dla Native SIP Trunking.
- Grupy Pick-Up.
- Obsługa wieloliniowości. System musi pozwalać na kreowanie zestawów wieloliniowych tak by pojedyncza rozmowa była sygnalizowana u wielu abonentów. Rozmowa musi być sygnalizowana na stanowisku optycznie i akustycznie.

- Obsługa wieloliniowości. System musi pozwalać na przypisanie linii jako pierwotnej do danego stanowiska, dodatkowej (pierwotnej na innym stanowisku), lub wirtualnej nie będącej pierwotnie przypisanej do żadnego stanowiska. Zależnie od trybu sygnalizacja akustyczna (dzwonienie) może być włączona, opóźniona lub wyłączona.
- Obsługa wieloliniowości. Dodatkowo system musi pozwalać na przypisanie linii jako pierwotnej, lub dodatkowej jako prywatnej (przypisanej wyłącznie do jednego stanowiska).
- System musi pozwalać na równoległe wykorzystanie wieloliniowej grupy wyszukiwania (multiline hunt grup) oraz usługi One number Service sterowanej przez CSTA. Softswitch musi przekazywać do serwera UC informacje pozwalające na rozróżnienie pomiędzy rozmowami automatycznie dystrybuowanymi w grupie i rozmowami nie skierowanymi do grupy.

- System musi posiadać możliwość grupowej i zdalnej konfiguracji terminali VoIP.
- System musi posiadać możliwość zdalnej aktualizacji oprogramowania terminali VoIP.
- System musi posiadać możliwość tworzenia kopii zapasowej konfiguracji terminali VoIP.
- System musi pozwalać na wykorzystanie kodu uwierzytelnienia pozwalającego na rozróżnienie rozmów prywatnych i służbowych dla danego użytkownika w danej grupie biznesowej.
- System musi dostarczać funkcjonalność powiadamiania alarmowego, o następujących parametrach:
  - Możliwość powiadamiania wszystkich użytkowników centrali
  - Liczba jednocześnie odtwarzanych komunikatów nie mniejsza niż 4
  - System musi umożliwiać dystrybucję wcześniej przygotowanych informacji słownych poprzez automatyczne wykonywanie połączeń na zdefiniowane numery telefonów, z kontrolą faktu odebrania połączenia. Musi istnieć możliwość zainicjowania rozgłoszenia przez użytkownika systemu z poziomu aparatu telefonicznego.
  - Aktywacja dystrybucji informacji słownej musi być możliwa z poziomu aparatu telefonicznego VoIP
  - System powiadamiania alarmowego musi zostać zintegrowany z systemem DSO Lotniska. Integracja musi umozliwiać w sposób automatyczny wysłanie informacji o wystąpieniu zagrożenia np. pożar.

- System musi pozwalać na generowanie trapów SNMP w przypadku wykonywania rozmów na numery alarmowe. Wygenerowany w takim przypadku event SNMP musi zawierać co najmniej: wybrany numer, identyfikację numeru dzwoniącego, ELIN/LIN, oznaczenie czasu.

Klawisze bezpośredniego wyboru stanowiska (DSS)

W środowisku pracy służb lotniskowych niezwykle istotna jest możliwość szybkiego kreowania połączeń za pomocą klawiszy bezpośredniego wyboru.

Funkcja bezpośredniego wyboru stanowiska (DSS) zapewnia dostęp użytkownika do poszczególnych funkcji dla określonego numeru wewnętrznego, poprzez użycie pojedynczego klawisza (klawisza DSS) z powiązaną z nim informacją o statusie..Klawisze DSS, mają inicjować bezpośrednie połączenia i posiadać możliwość użycia funkcji .Oba typy funkcji klawiszy DSS musza znajdować się w obrębie grupy biznesowej użytkownika, i nie być współdzielone pomiędzy grupami biznesowymi. Dla jednego urządzenia (aparatu) należy umożliwić przydzielenie do dziewięciu klawiszy DSS.

W ramach systemu przewiduje się realizację układów Sekretarsko/Dyrektorskich

Zostaną zastosowane następujące usługi:

- Dyrektor:
- Klawisz wyboru linii
- Klawisz odrzucenia rozmowy
- Linia prywatna
- Sprawdzenie linii (do każdego Sekrearza)
- Klawisz powtarzania wybierania
- Klawisz bezpośredniego wyboru (DSS-D do każdego dyrektora)
- Klawisze Wł/Wył przeniesienie dzwonienia
- Sekretarz:
- Klawisz wyboru linii
- Klawisz wyboru linii (innego Sekretarza)
- Dzwonienie z inną identyfikacją (w imieniu każdego Dyrektora i Sekretarza)
- Klawisz powtarzania wybierania (do każdego Dyrektora i Sekretarza)
- Klawisz dzwonka
- Klawisz zastępstwo
- Sprawdzenie linii (do każdego Dyrektora)
- Klawisz powtarzania wybierania

- Sprawdzenie aktualnie wybranej linii
- Połączenia przychodzące do Dyrektora są bezpośrednio przekierowane na telefon Sekretarza.
- Sekretarz może zawsze monitorować wszystkie połączenia przychodzące do Dyrektora są bezpośrednio przekierowane na telefon Sekretarza.
- Sekretarz może zawsze monitorować wszystkie połączenia przychodzące do Dyrektora za pośrednictwem klawiszy linii i odpowiednio zareagować.
- Dostępne będą następujące konfiguracje dla Dyrektorów i Sekretarzy:
- 1x Dyrektor i 1x Sekretarz
- 2x Dyrektorzy i 1x Sekretarz
- 2x Dyrektorzy i 2x Sekretarz:
- Bezpośrednie powiązanie Dyrektor 1- Sekretarz 1 oraz Dyrektor 2- Sekretarz
- Jeśli jeden z Sekretarzy nie jest obecny, drugi Sekretarz może działać w jego zastępstwie
- 4x Dyrektorów i 2x Sekretarze
- Bezpośrednie powiązanie Dyrektorzy 1+2 do Sekretarz 1 i Dyrektorzy 3+4 do Sekretarz 2
- Jeśli jeden z Sekretarzy nie jest obecny, drugi Sekretarz może działać w jego zastępstwie

System zunifikowanej komunikacji obsługiwał będzie różne służby lotniskowe, konieczna jest więc możliwość wirtualnego podziału systemu komunikacji głosowej na podsystemy(grupy biznesowe) dla poszczególnych służb. Wymagane jest aby system wspierał niezależną obsługę wydzielonych podsystemów.

Moduły do obsługi łączy miejskich

Do analizy, na potrzeby projektu przywołano konkretny system: mozna użyć rozwiązania równoważnego.

- Wykonawca dostarczy moduł bramy: ISDN 30B+D, do podłączenia łączy miejskich z sygnalizacją Euro ISDN.
- Powyższe moduły muszą pochodzić od producenta systemu i być objęte wspólnym zarządzaniem.
- Urzadzenie musi zapewniać funkcje SBC - moduł zabezpieczenia łączy SIP trunk (Session Boarder Controller) umożliwiające przyłączenie do operatora publicznego za pomocą SIP trunk.

System taryfikacyjny

- System musi skalować się do obsługi co najmniej 200 numerów jedynie poprzez zakup odpowiedniej licencji.
- Oprogramowanie systemu musi być wykonane w oparciu o centralną, relacyjną, komercyjną bazę danych SQL.
- Możliwość importu rekordów taryfikacyjnych według zadanego harmonogramu, aplikacja do pobierania danych powinna mieć możliwość pracy, jako usługa systemowa.
- Funkcja ręcznego importu rekordów taryfikacyjnych (na żądanie).
- System powinien posiadać architekturę, która pozwala na elastyczne jego dostosowanie do potrzeb użytkowników uwzględniające wewnętrzne zmiany organizacyjne, zmiany kadrowe, zmiany operatorów telekomunikacyjnych, itp. Wszystkie konieczne zmiany w systemie, wynikające z powyższego powinny być możliwe do wykonania samodzielnie przez operatora lub administratora systemu bez angażowania Wykonawcy. Procedura takich zmian musi zostać opisana w dokumentacji systemu.
- Dostęp operatora systemu powinien odbywać się poprzez wbudowany system autoryzacji, umożliwiający definiowanie różnych poziomów uprawnień dla użytkowników systemu.
- Pobieranie danych taryfikacyjnych z systemu SoftSwitch winno odbywać się w trybie automatycznym wg ustalonego scenariusza lub ręcznie wg potrzeb przy wykorzystaniu dostępnych interfejsów, a następnie wykonywane jest przetwarzanie rekordów do jednolitego formatu i gromadzenie w centralnej bazie danych.
- Prezentacja aktualnej informacji o stanie pobierania i przetwarzania rekordów.
- Automatyczne informowanie o pojawieniu się rekordów taryfikacyjnych generowanych przez nowych abonentów, linie zewnętrzne i kody PIN w momencie pierwszego pojawienia się ich w systemie.
- Polskojęzyczny interfejs operatora. Wszystkie moduły oprogramowania muszą mieć interfejs użytkownika w języku polskim z poprawną wizualizacją, edycją, sortowaniem i drukowaniem wyrazów z polskimi znakami narodowymi.
- Zapewnienie możliwości rekalkulacji kosztów połączeń po zmianie cenników usług telekomunikacyjnych. Rekalkulacja musi uwzględniać historię przypisania abonentów do struktury organizacyjnej oraz historię zmian w tej strukturze.

- Umożliwienie dokonywania zmian w strukturze organizacyjnej i zmian w przyporządkowaniu numerów wewnętrznych i kodów PIN z zachowaniem poprzednio przypisanych danych bez konieczności archiwizacji.
- Zachowanie historii połączeń dla nieaktywnego numeru wewnętrznego.
- Umożliwienie przeprowadzania obliczeń symulacyjnych na rzeczywistych rekordach poprzez definiowanie różnych taryf w celu porównania ofert operatorów.
- Wyeliminowanie możliwości dublowania się połączeń (kosztów połączeń) rejestrowanych jednocześnie w różnych węzłach sieci.
- Narzędzia do zaawansowanego filtrowania sortowania, wyszukiwania rekordów taryfikacyjnych wg dowolnie zadanych kryteriów (dowolny zakres czasowy, dowolny zakres numerów wewnętrznych, dowolnej grupy operatorów). Prezentacja rekordów w postaci tabelarycznej z możliwością edycji wyglądu pól (kolejności, szerokości, pokazywania lub ukrywania ich na liście) oraz ich zapis, wydruk i eksport do formatów: TXT, XLS, HTML, PDF.
- System musi umożliwiać definiowanie automatycznie generowanych raportów rozsyłanych za pomocą poczty elektronicznej.
- System musi umożliwiać dostęp do danych taryfikacyjnych przez interfejs WWW dla każdego użytkownika w tym samym czasie.
- Administrator musi mieć możliwość przydzielania uprawnień dla dostępu do danych dla poszczególnych użytkowników lub grup użytkowników interfejsu WWW.
- Raportowanie w interfejsie WWW z możliwością wykreowania dowolnej formy zestawienia danych, wykonania statystyk ruchu i wykresów z użyciem kreatora raportów.
- System powinien posiadać funkcje umożliwiające ciągły nadzór i monitorowanie kompletności pobranych danych do jednorodnej bazy danych z rozbiciem na poszczególne systemy.
- System powinien umożliwiać przeglądanie logów systemowych oraz monitorować zagrożenia procesu zbierania danych taryfikacyjnych.
- Możliwość wprowadzenia numeru w systemie taryfikacji, jeżeli nie ma przyznanego abonamentu i nie były realizowane rozmowy z tego numeru.
- Możliwość prezentacji raportu w formie graficznej, np. wykresu.
- Wymagana jest zdolność do taryfikacji połączeń przychodzących, wychodzących, wewnętrznych, transferowych.

- Wymagany jest mechanizm kontroli kosztów z podziałem na osoby, grupy osób i typy połączeń, możliwość tworzenia raportów na LW zdefiniowanych jednocześnie w więcej niż jednej strukturze organizacyjnej.
- Archiwizacja i zabezpieczenie danych na nośnikach zewnętrznych (zapis na CD, DVD itp.).
- Łącze między centralą softswitch a systemem taryfikacji musi być realizowane za pomocą połączenia IP.
- Dostęp do systemu musi być realizowany przez interfejs WWW oraz w trybie graficznym za pomocą dedykowanej aplikacji instalowanej na komputerze.
- Możliwość ręcznego lub automatycznego importu danych o taryfikowanych obiektach (np. linie wewnętrzne, użytkownicy) z pliku zewnętrznego, kompatybilnego z aplikacją Microsoft Excel.
- Oprogramowanie musi być gotowe do udostępnienia funkcjonalności blokowania linii wewnętrznej po przekroczenia określonego limitu kwotowego za połączenia.
- System musi być kompletny, tj. posiadać wszystkie niezbędne elementy sprzętowe i programowe i licencyjne.
-

System poczty głosowej

- System poczty głosowej musi pochodzić od tego samego producenta, co system Softswitch. Dopuszcza się zastosowanie rozwiązania równoważnego certyfikowanego przez producenta systemu Softswitch.
- System musi zapewnić 50 skrzynek poczty głosowej i umożliwiać rozbudowę do 200 skrzynek. Każda ze skrzynek poczty głosowej musi pozwalać na przechowywanie co najmniej 10 wiadomości o długości 3 minuty każda.
- wiadomości głosowej za pomocą dedykowanej diody LED aparatu telefonicznego oraz za pomocą wiadomości e-mail.
-

System obsługi faksów

- System faks serwerowy musi pochodzić od tego samego producenta, co istniejący system Softswitch. Dopuszcza się zastosowanie rozwiązania równoważnego certyfikowanego przez producenta systemu Softswitch.
- System musi zapewnieć 50 i pozwalać na rozbudowę do co najmniej 200 skrzynek faksowych jedynie poprzez zakup dodatkowych licencji. Rozbudowa ta nie może w sposób zauważalny dla użytkowników pogorszyć parametrów wydajnościowych systemu.

- Wymagana obsługa protokołu T.38.
- System musi integrować się z dowolnym systemem e-mailowym (przesyłanie faksów na skrzynkę użytkownika przez wiadmomość email).
- System musi umożliwiać wysyłanie faksów z poziomu dokumentu programu – za pomocą dedykowanej wtyczki programowej.
- Serwer musi oferować możliwość archiwizacji faksów przychodzących i wychodzących.
- Zarządzanie systemem musi być realizowane co najmniej za pomocą interfejsu www.
- Faks Serwer musi być kompletny, tj. posiadać wszystkie niezbędne elementy sprzętowe, programowe i licencyjne.

System zunifikowanej komunikacji(UC)

- Wymagana jest, dostawa 50 licencji aplikacji (UC)

System musi zapewniać:

- Sterowanie/Administracja/Filtrowanie połączeń (CTI)
- Szyfrowanie sygnalizacji
- Zarządzanie kontaktami oparte na serwerze
- Dziennik połączeń oparty na serwerze
- Poczta głosowa
- Usługa Jednego Numeru (ONS)
- Zarządzanie preferowanym urządzeniem z uwzględnieniem listy urządzeń
- Przekazywanie aktualnej rozmowy na jedno z preferowanych urządzeń (ad-hoc handover)
- Portal głosowy z dostępem do funkcji UC
- Zawansowane wielopoziomowe zarządzanie dostępnością osobistą użytkownika, dostępnością mediów i lokalizacji
- Konferencje ad-hoc
- Oddzwonienie multimedialne "Tell-Me-When" - automatyczne notyfikacje i połączenia oparte na statusie dostępności
- Zarządzanie komunikacją oparte o reguły
- Pokoje konferencyjne (zaplanowane konferencje stałe lub typu Meet-Me)
- Konferencje moderowane (jeden lub więcej moderatorów) i otwarte (bez moderatora)
- Zarządzanie konferencjami w oparciu o role

Ograniczenia dla funkcji telefonicznych

Poniższe usługi telefonicznej nie będą wykorzystywane dla użytkowników korzystających z usług zunifikowanej komunikacji:

- Grupy odbierania połączeń przy dzwonku nocnym
- Hot Desking (zamiast tego należy użyć funkcje UC)
- Grupy poszukiwania (hunting)
- Przekierowanie połączeń (funkcje UC takie jak na przykład reguły muszą być użyte zamiast przekierowania połączeń)
- Wstrzymanie połączenia (hold) dla urządzeń MGCP
- Funkcje odrzucenie z zakończeniem połączenia
- Funkcja nie przeszkadzać
- Selektywne przyjęcie / odrzucenie rozmowy (funkcja UC, taka jak reguły powinna być użyta zamiast tej funkcji)
- Grupa dzwonienia szeregowego (funkcja UC taka jak na przykład Lista Urządzeń musi być użyta zamiast tej funkcji)
- Dzwonienie równoległe
- Aktywacja Zdalna
- Grupa poszukiwania MLHG jako Użytkownik systemu Softswitch

Terminale końcowe

Telefon podstawowy VoIP

- Obsługa protokołu SIP (RFC 3261).
- Minimum 3 programowalne (predefiniowane) klawisze funkcyjne z diodami LED.
- Minimum 3 stałe klawisze funkcyjnych z diodami LED
- Gniazdo zestawu nagłownego
- Minimum 4 klawisze do regulacji głośności i obsługi zestawu nagłownego.
- Minimum 3 kierunkowy klawisz nawigacyjny i klawisz potwierdzenia
- Możliwość montażu na ścianie.
- Optyczna sygnalizacja dzwonienia (LED)
- Wyświetlacz dwuliniowy 2x 34 znaki
- Podstawa umożliwiająca ustawienie telefonu pod czterema różnymi kątami
- Podłączenie w standardzie Ethernet 10/100/1000 Base-T.
- Wsparcie dla kodeków audio: G.729AB, G.722, G711.
- Wsparcie dla 802.1Q, 802.1p, DiffServ.

- Wsparcie przypisania adresu centralnego systemu zarządzania telefonami za pomocą opcji DHCP.
- Wsparcie przypisania do numeru VLAN za pomocą opcji DHCP.
- Wsparcie przypisania adresu SIP Registrar w Softswitch za pomocą usługi DNS-SRV
- Wsparcie przypisania adresu podstawowego i zapasowego SIP Registrar w Softswitch
- Zasilanie za pomocą sieci LAN w klasie 2.

Telefon zaawansowany VoIP:

- Obsługa protokołu SIP (RFC 3261).
- Kolorowy (16bit) wyświetlacz graficzny TFT o rozdzielczości minimum 320 x 240, przekątna co najmniej 5 cali.
- Możliwość zasilenia w standardzie PoE IEEE 802.3af class 3 lub poprzez zewnętrzny zasilacz
- Optyczna sygnalizacja dzwonienia (LED).
- Minimum 8 stałych klawiszy funkcyjnych z diodami LED.
- Minimum 8 programowalnych klawiszy funkcyjnych z diodami LED.
- Minimum 4 kierunkowy klawisz nawigacyjny i klawisz potwierdzenia
- Minimum 4 klawisze kontekstowe.
- Rozmowy za pomocą zestawu głośnomówiącego (full duplex).
- Gniazdo słuchawek nagłownych.
- Możliwość montażu na ścianie.
- Możliwość podłączenia minimum dwóch dodatkowych modułów klawiszy.
- Mikroswitch Ethernet 10/100/1000 Base-T.
- Wsparcie dla kodeków audio: G.729AB, G.722, G711.
- Wsparcie dla 802.1Q, 802.1p, DiffServ.
- Wsparcie LLDP-MED.
- Wsparcie przypisania adresu centralnego systemu zarządzania telefonami za pomocą opcji DHCP.
- Wsparcie przypisania do numeru VLAN za pomocą opcji DHCP.
- Wsparcie przypisania adresu SIP Registrar w Softswitch za pomocą usługi DNS-SRV
- Wsparcie przypisania adresu podstawowego i zapasowego SIP Registrar w Softswitch
- Dostęp do katalogowej skrzynki kontaktów (Klient LDAP).
- Obsługa aplikacji XML
- Szybkie wyszukiwanie i zaawansowane wyszukiwanie z różnymi kryteriami wyszukiwania.

- Zasilanie za pomocą sieci LAN w klasie 2.

Telefon dyspozytorski VoIP:

- Obsługa protokołu SIP (RFC 3261).
- Kolorowy (16bit) wyświetlacz graficzny TFT o rozdzielczości minimum 320 x 240 ,przekątna co najmniej 5 cali.
- Możliwość zasilenia w standardzie PoE IEEE 802.3af class 3 lub poprzez zewnętrzny zasilacz
- Optyczna sygnalizacja połączenia.
- Minimum 8 stałych klawiszy funkcyjnych z diodami LED.
- Minimum 8 programowalnych klawiszy funkcyjnych z diodami LED.
- Minimum 4 kierunkowy klawisz nawigacyjny i klawisz potwierdzenia
- Minimum 4 klawisze kontekstowe.
- Rozmowy za pomocą zestawu głośnomówiącego (full duplex).
- Słuchawki nagłowne
- Mikroswitch Ethernet 10/100/1000 Base-T.
- Wsparcie dla kodeków audio: G.729AB, G.722, G711.
- Wsparcie dla 802.1Q, 802.1p, DiffServ.
- Wsparcie LLDP-MED.
- Wsparcie przypisania adresu centralnego systemu zarządzania telefonami za pomocą opcji DHCP.
- Wsparcie przypisania do numeru VLAN za pomocą opcji DHCP.
- Wsparcie przypisania adresu SIP Registrar w Softswitch za pomocą usługi DNS-SRV
- Wsparcie przypisania adresu podstawowego i zapasowego SIP Registrar w Softswitch
- Dostęp do katalogowej skrzynki kontaktów (Klient LDAP).
- Obsługa aplikacji XML
- Szybkie wyszukiwanie i zaawansowane wyszukiwanie z różnymi kryteriami wyszukiwania.
- Telefon musi zostać zintegrowany z systemem FIS. Na wyświetlaczu musi zostać wyświetlona informacja w postaci tabeli o przylotach i odlotach samolotów.
- Każdy aparat dyspozytorski należy wyposażyć w przystawki klawiszowe zapewniające obsługę przez urządzenie łącznie co najmniej 30 funkcyjnych klawiszy programowalnych z wyświetlaczami opisów klawiszy i diodą sygnalizacyjną LED dla każdego klawisza.

Telefon bezprzewodowy DECT

- Wyświetlacz kolorowy minimum 128x160 pikseli

- Podświetlana klawiatura
- Przycisk trybu głośnomówiącego
- Klawisz blokady klawiatury
- Funkcje klawisza odbierania rozmów:
  - przytrzymany krótko: lista ponownego wybierania
  - gdy wciśnięty: status wybierania
- Przycisk wyciszenia mikrofonu
- Książką kontaktów min 500 wpisów
- Obsługa sieci DECT: Roaming, Handover, Komunikat ostrzegający na wyświetlaczu przy wychodzeniu ze stref zasięgu sieci DECT
- Słuchawka musi być dostarczona razem z ładowarką

Wymagania ilościowe przedstawiono w tabeli w rozdziale 1.

Infolinia lotniskowa

System musi posiadać funkcje pozwalająca na uruchomieni infolinii informującej pasażerów o zasadach obsługi, zasadach bezpieczeństwa i innych komunikatach pozwalających na usprawnienie obsługi ruchu. Określa się następujące wymagania funkcjonalne:

- Inteligentny ruting kontaktów dla kontaktów głosowych
- Decyzje rutingowe na zasadzie źródło/cel dzwoniącego
- Ruting oparte na grupie z agentami w pojedynczych lub licznych grupach
- Zbiorcza obsługa kontaktów (MCH)
- Ruting oparty na umiejętnościach dla kontaktów głosowych
- Wiadomości informacyjne dla pasażerów w celu zautomatyzowania elementów samoobsługowych np. godzin pracy, cotygodniowych informacji i często zadawanych pytań,
- Zbieranie wymagań poprzez pozwalanie klientom na wybranie opcji i przechodzenie do kolejnych menu poprzez ich klawiaturę telefoniczną. Takie interaktywne menu pozwala klientowi dokonać wyboru podczas czekania w kolejce i może być skonfigurowane tak, aby mozna je było przerwać i dokonać wyboru zanim dane prośby skończą się wyświetlać.
- Raporty pracy infolinii – ilość połączeń odebranych /nieodebranych/czas oczekiwania w kolejce

System IP DECT

Komunikację bezprzewodową należy zapewnić na terenie całego Lotniska poprzez instalację stacji bazowych DECT . Przewiduje się instalację 4 stacji bazowych DECT na każdą kondygnację oraz trzech stacji zewnętrznych obsługujących część płyty. Stacje bazowe muszą komunikować się z serwerem IP DECT i systemem komunikacyjnym poprzez Sieć IP. Rozwiązanie DECT musi stanowić spójny system z serwerem Softswitch SIP (musi pochodzić od tego samego producenta, dopuszcza się zastosowanie rozwiązania równoważnego, certyfikowanego przez producenta systemu softswitch). System musi zapewniać handover pomiędzy stacjami. Przewiduję się uruchomienie 20 słuchawek DECT.

Zestawienie materiałów

Do analizy, na potrzeby projektu przywołano konkretny system: można użyć rozwiązania równoważnego. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

zastosowanie	grupa produktu	numer	opis produktu	ilość
Przełączniki dostępowe	B-Series	B5K125-48P2	B5 (48) 10/100/1000 AT-POE RJ45 ports, (2) combo SFP ports, (2)10G ports, (2) dedicated stacking ports and external RPS connector	6
	B-Series	B5K125-24P2	B5 (24) 10/100/1000 AT-POE RJ45 ports, (2) combo SFP ports, (2)10G ports, (2) dedicated stacking ports and external RPS connector	7
	C-Series	STK-CAB-SHORT	30CM STACKING CABLE - B and C Series	6
Przełączniki szkieletowe	S-Series	S4-CHASSIS	S-Series S4 Chassis and fan tray (Power supplies ordered separately)	2
	S-Series	SK5208-0808-F6	S-Series S155 Class I/O-Fabric Module, 1280Gbps Load Sharing - 8 Ports 10GBASE-X via SFP+ and two Type2 option slots (Used in S1/S4/S6/S8)	2
	S-Series	SOT2206-0112	S-Series Option Module (Type1) - 12 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) (Compatible with Type1 & Type2 option slots)	2
	S-Series	S-AC-PS	S-Series AC power supply, 20A, 100-240VAC input, (1200/1600W) (For use w/ S3/S4/S6/S8)	4
	S-Series	S1-CHASSIS-A	S-Series S1 Chassis and fan tray. Compatible with Fabric Modules only. (SSA 1000W Power supplies ordered separately)	2
	S-Series	SK5208-0808-F6	S-Series S155 Class I/O-Fabric Module, 1280Gbps Load Sharing - 8 Ports 10GBASE-X via SFP+ and two Type2 option slots (Used in S1/S4/S6/S8)	2
	S-Series	SOT2206-0112	S-Series Option Module (Type1) - 12 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) (Compatible with Type1 & Type2 option slots)	2
	S-Series	SSA-AC-PS-1000W	S-Series Standalone (SSA S130 and S150 Class) and S1-Chassis - AC and PoE power supply, 15A, 110-240VAC input, (1000/1200W)	4
wkładki Fo	XFP	10GB-LRM-SFPP	10 Gb, 10GBASE-LRM, IEEE 802.3 MM, 1310 nm Long Wave Length, 220 M, LC SFP+	28

zastosowanie	grupa produktu	numer	opis produktu	ilość
AP	Wireless	WS-AP3710i	DUAL RADIO 3X3:3 MIMO INTEGRATED ANTENNA	10
	Wireless	WS-V2110-8-ROW	V2110 Virtual Wireless Gateway for Rest-of-World (verify country availability before ordering). Base of 8 APs, expandable to 248 APs via capacity upgrades (WS-APCAP-1, WS-APCAP-16).	1
	Wireless	WS-RADAR-1	Radar capacity for C25 and V2110. Adds Radar capacity for 1 access point.	6
	Netsight	NAC-VB-20	Includes four virtual NAC Gateways each supporting up to 500 end systems and available add-on assessment license	1
	Netsight	NMS-ADV-25	NetSight Advanced License for up to 25 devices and 250 thin Aps	1
	Security Appliances	DSIMBA7-GB	ALL-IN-ONE SIEM APPLIANCE (200 EPS)	1
Firewall		PA3050	Palo Alto 3050	2
Cordless	OpenScape	L30280-F600-A183	HiPath Cordless IP V1 - Base Station BSIP1	1
	OpenScape	L30280-F600-A185	BSIP1 Base Station License for HiPath Cordless IP V1	11
	OpenScape	L30280-F600-A186	HiPath Cordless IP V1 Server License	1
	OpenScape	L30280-F600-A187	HiPath Cordless IP V1 Software CD	1
	OpenScape	L30280-B600-B212	Outdoor Housing for BS4 (Neutral), BSIP1without Heating	3
	OpenScape	L30251-U600-A395	EIC Code (DECT Code)	1
	OpenScape	L30280-Z600-F105	Mains Power Cord with Straight Appliance Connector, EURO Variant	2
podsystem alarmowania	OpenScape	L30280-D600-A750	OpenScape Alarm Response - Economy (OScAR-Eco) Server V1	1
	OpenScape	L30280-D600-A753	OScAR-Eco Serial Port Kit	1
centrala SIP/UC	OpenScape	L30280-A622-A137	Base Package "Enterprise" (OSV)	1
	OpenScape	L30280-A600-A178	Software CD	1

zastosowanie	grupa produktu	numer	opis produktu	ilość
IVR	OpenScape	L30280-A622-A196	Base Call Director SIP Service License	1
	OpenScape	L30280-A622-A187	1 Port Call Director SIP Service License	5
Poczta faks i głos	OpenScape	L30280-D600-D50	OpenScape Xpressions V7 SW incl. Documentation USB Stick	1
	OpenScape	L30280-D622-D52	OpenScape Xpressions V7 Base License (excl. Connectors)	1
	OpenScape	L30280-D622-D58	OpenScape Xpressions V7 Voice License	50
	OpenScape	L30280-D622-D62	OpenScape Xpressions V7 Unified License	50
	OpenScape	L30280-D622-D74	OpenScape Xpressions V7 Mediastreaming 1-Port License for Voice/Unified	3
Telefony	OpenScape	L30250-F600-C141	Zasilacz do optiPoint 410/420/Openstage	100
	OpenScape	L30250-F600-C271	LAN Cable (CAT6), 4m	150
	OpenScape	L30250-F600-C280	OpenScape Desk Phone IP 35G	50
	OpenScape	L30250-F600-C281	OpenScape Desk Phone IP 55G	50
	OpenScape	L30250-F600-C283	LAN Cable 25cm	50
	OpenScape	L30250-F600-C284	Stencilled Labels for OpenScape Desk Phone IP 35G	50
	OpenScape	iTar 300	iTar do 300 abonentów	1
	OpenScape	iTar-Kolektor	iTar kolektor danych FTP	1
	OpenScape	KOMP_DRUK	Drukarka Laserowa	1
UC	OpenScape	L30280-D600-H131	OpenScape Voice and OpenScape UC Application Enterprise Edition Package V7 SW	1

zastosowanie	grupa produktu	numer	opis produktu	ilość
VoIP	OpenScape	L30220-D622-A470	OpenScape Voice V7 Base Package License	1
	OpenScape	L30220-D622-A472	OpenScape Voice V7 Dynamic User License	100
	OpenScape	L30280-D622-H16	OpenScape Personal Edition V7 Base License for SIEL	1
	OpenScape	L30280-Z622-A613	SESAP Service License On Loan, 3-Year Term	1
	OpenScape	L30280-Z622-A610	DVD with SESAP Software Suite On Loan	1
	OpenScape	L30258-W622-D681	OpenScape Fusion V1 for MS Outlook Base License	1
	OpenScape	L30280-D600-H160	OpenScape UC Application Enterprise Edition V7 SW for existing SEN platforms	1
	OpenScape	L30280-D622-H162	OpenScape UC Application Enterprise Edition V7 Base License For existing SEN platforms	1
	OpenScape	L30280-D622-H166	OpenScape Enterprise Edition V7 User License	50
	OpenScape	L30280-D622-H173	OpenScape V7 Audio Conference Channel	8
	OpenScape	L30220-D600-A246	OpenScape Voice - IBM Application Server Typ 1 x3250 M3	4
	OpenScape	L30280-Z600-F100	Mains Power Cord with Right-Angled Appliance Connector, EURO Variant	4
	IBM	IBM PL_7915E3G_Cfg1	IBM PL OpenScape UC Virtualisation Server-IBM x3650 M4	2
	IBM	IBM PL_SESAP order Win2k3S Extra	IBM PL OpenScape Application Server Typ 1 x3250 - SESAP	1
Brama do TDM	OpenScape		OpenScape Branch V2	20
	OpenScape		OpenScape Branch V7	10
	OpenScape	L30220-D600-A565	OpenScape Branch 50i A024 V2/V7 Server	1
	OpenScape	L30220-D600-A571	OpenScape Branch 500i DP4 V2/V7 Server	1
	OpenScape	L30220-D600-A573	Patch Panel 24 ports for OpenScape Branch 50i	1

	OpenScape	L30220-D600-A574	Centronic Cable 24 Pair for OpenScape Branch 50i	1
	OpenScape	L30220-D622-A621	OpenScape Branch V7 Base License	2
	OpenScape	L30280-Z600-F105	Mains Power Cord with Straight Appliance Connector, EURO Variant	2
	OpenScape	L30250-F600-A842	LAN Cable (CAT5), 4m	2
Zarządzanie tel. VoIP	OpenScape	L30280-D622-F696	OpenScape Deployment Service V7 Basic User License	1000
	OpenScape	L30280-D622-F697	OpenScape Deployment Service V7 Base System License	1
	OpenScape	L30280-D622-C700	OpenScape Fault Management V7 Base Package	1
	OpenScape	L30280-D622-C701	OpenScape Fault Management V7 Port License	200
	Usługi	Serwis_Montaż	Wdrożenia	221
	Usługi	Serwis_AudytIPDA	Audyt sieci LAN/WAN dla VoIP	1
	Usługi	Serwis_AudytVM	Audyt infrastruktury dla wirtualizacji	1
	Usługi	Serwis_CotB	Integracja usługi katalogowej LDAP w środowisku Klienta	1
	Usługi	Serwis_SSO	Logowanie do UC hasłem domenowym Windows (SSO dla 1 rodzaju klienta)	1
SWA	Usługi	L30220-S632-L987	OSC SWA for OSC Xpressions Base	2
	Usługi	L30280-D601-B295	OSC SWA for OSC Xpressions Voice	100
	Usługi	L30280-D601-B296	OSC SWA for OSC Xpressions Unified	100
	Usługi	L30220-S632-L974	OSC SWA for OSC UC Application Enterprise Edition for existing SEN platforms (per year and Base)	2
	Usługi	L30220-S632-L959	OSC SWA for OSC UC Appl User License (per year and user)	100
	Usługi	L30220-S632-L958	OSC SWA for OpenScape Voice Conference Channel (per year and Channel)	16
	Usługi	L30220-S632-L960	OSC SWA for OSC Voice Base System	2
	Usługi	L30220-D601-A301	OSC SWA for OSC Voice Dynamic User	400
Usługi OUCS	Usługi	OUCS_SOW	Warstat OpenScale: Scope of Work Definition	1
	Usługi	PL_L30258-W633-C535	OpenScale: Solution Acceptance Testing (OSRA) 1 day	3

Do analizy, na potrzeby projektu przywołano konkretny system: można użyć rozwiązania równoważnego. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Systemy bezpieczeństwa obiektu

Podstawowym aktem prawnym regulującym zasady wykonywania zadań ochrony osób i mienia jest Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (DzU 2005, nr 145, poz. 1221, Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 lipca 2005 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie osób i mienia). W artykule pierwszym wspomniana ustawa określa między innymi obszary, obiekty i urządzenia podlegające obowiązkowej ochronie. Zgodnie z nią obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa podlegają obowiązkowej ochronie przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenia techniczne.

Podstawowym aktem prawnym, który określa organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania w tej dziedzinie, a także zasady finansowania zadań zarządzania kryzysowego jest Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU 2007, nr 89, poz. 590 z poźn. zm.). W artykule 3. pkt 2. tej ustawy pod pojęciem infrastruktury krytycznej należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Infrastruktura krytyczna wśród wielu innych wymienionych w ustawie obejmuje również systemy transportowe i komunikacyjne, między innymi porty lotnicze.

Na podstawie art. 187. ust. 1. Ustawy o ochronie osób i mienia wydano akt wykonawczy w postaci Rozporządzenia Rady Ministrów z dnia 19 czerwca 2007 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego realizującego zasady ochrony lotnictwa (DzU 2007, nr 116, poz. 803). W paragrafie 2.1. zapisano, że za działania podejmowane w ramach Krajowego Programu odpowiada między innymi zarządzający lotniskiem. Do najważniejszych obiektów infrastruktury portowej podlegających szczególnej ochronie należy zaliczyć:

1) terminal pasażerski i inne terminale;
2) wieżę kontroli ruchu lotniczego;
3) generatory energetyczne;
4) magazyny paliw i smarów;
5) systemy klimatyzacyjne i wentylacyjne;
6) bocznice kolejowe;

7) ujęcia wody;
8) płyty postojowe statków powietrznych;
9) hangary;
10) inne urządzenia lub obiekty uznane przez prezesa Urzędu Lotnictwa Cywilnego lub zarządzającego lotniskiem za kluczowe dla ochrony lotnictwa cywilnego przed aktami bezprawnej ingerencji (np. oświetlenie ścieżki podejścia, urządzenia ILS[1] itp.).

Już na etapie projektowania zarządzający lotniskiem uzyskuje opinię prezesa ULC o planie systemu ochrony terminali pasażerskich, towarowych oraz innych obiektów znajdujących się w sąsiedztwie strefy zastrzeżonej lotniska, przed rozpoczęciem ich budowy lub rozbudowy, zwłaszcza w zakresie:

- działań mających na celu ochronę pasażerów, bagażu kabinowego i rejestrowanego, w tym ich identyfikację;
- działań mających na celu ochronę ładunków, przesyłek ekspresowych i kurierskich, poczty i zaopatrzenia pokładowego;
- sposobu dokonywania kontroli dostępu do stref zastrzeżonych;
- wykorzystania sprzętu specjalistycznego.

Następnie zarządzający lotniskiem wyznacza strefy zastrzeżone lotniska oraz ich części krytyczne, a także przejścia do tych stref. Strefy i przejścia, o których mowa, wyznacza się w uzgodnieniu ze Strażą Graniczną, Policją, Służbą Celną oraz prezesem ULC. Zarządzający lotniskiem określa je w programie ochrony lotniska.

Za ochronę strefy zastrzeżonej lotniska, w tym prowadzenie kontroli bezpieczeństwa osób i pojazdów wjeżdżających do niej, odpowiada zarządzający lotniskiem przy pomocy służby ochrony lotniska. Obiekty chronione są przy zastosowaniu osobowych i technicznych środków ochrony oraz podlegają patrolowaniu przez służbę ochrony, przy czym technika i taktyka pełnienia służby jest określana w planie ochrony uzgadnianym z właściwym terytorialnie komendantem Policji.

Obiekty portu lotniczego chroni się ze względu na występujące zagrożenia naturalne oraz te wywołane przez człowieka. Do zagrożeń naturalnych (obiektywnych) należą anomalie pogodowe oraz inne czynniki naturalne uniemożliwiające eksploatację lotniska, w tym:

- gwałtowne porywy wiatru, tzw. trąby powietrzne;
- lewne opady deszczu, wyładowania atmosferyczne;
- obfite opady śniegu i zamiecie śnieżne;
- zaleganie mgieł (przy ograniczeniu widoczności poniżej 600 m);
- zagrożenie powodziowe;
- obfite opady śniegu i zamiecie śnieżne lub inne anomalie atmosferyczne.

Do zagrożeń wywołanych przez człowieka należą:

- bezprawne wtargnięcie do strefy zastrzeżonej;
- bezprawne wniesienie do strefy zastrzeżonej przedmiotów zabronionych wymienionych w Obwieszczeniu nr 5 Prezesa Urzędu Lotnictwa Cywilnego dnia 9 sierpnia 2007 r. w sprawie listy przedmiotów zabronionych do wnoszenia na teren strefy zastrzeżonej lotniska i przewozu w bagażu kabinowym oraz rejestrowanym pasażera (Dz.Urz. ULC, nr 5 z 01.10.2007 r.);
- podłożenie bądź zagrożenie podłożenia materiałów i urządzeń wybuchowych w obiektach i urządzeniach portu lotniczego;
- użycie bądź zagrożenie zastosowania bioterroryzmu bądź tzw. brudnej bomby;
- atak zbrojny na osoby przebywające w obiektach portu lotniczego;
- wniesienie na pokład samolotu urządzenia wybuchowego bądź przedmiotów zabronionych do przewozu drogą lotniczą;
- wzięcie zakładników na obszarze portu lotniczego;
- zawładnięcie samolotem (z pasażerami bądź bez pasażerów);
- lądowanie w porcie lotniczym samolotu z terrorystami na pokładzie;
- akty sabotażu bądź dywersji;
- akty o charakterze kryminalnym;
- zakłócenia porządku publicznego;
- akty wandalizmu, w tym niszczenie mienia

Za całokształt funkcjonowania portu lotniczego, realizację procedur kontrolnych i respektowanie międzynarodowych standardów i uregulowań prawnych, jakie polska władza, w tym władza lotnicza, zobowiązała się przestrzegać i stosować, odpowiadają władze portu lotniczego reprezentowane przez zarząd. Jest on w rozumieniu artykułu 7.1 wspomnianej Ustawy o ochronie osób i mienia tzw. kierownikiem jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami. Jako zarządzający lotniskiem[2] jest on również odpowiedzialny za zorganizowanie oraz nadzór nad działaniami mającymi na celu ochronę lotniska przed atakami bezprawnej ingerencji. W tym względzie zarząd zobowiązany jest między innymi do:

- wyznaczenia osoby legitymującej się odpowiednim poświadczeniem bezpieczeństwa, która będzie odpowiedzialna za ochronę lotniska i szkolenie w tym zakresie osób zatrudnionych na lotnisku;
- opracowania, w porozumieniu ze Strażą Graniczną (SG), Policją oraz Służbą Celną, tzw. Programu Ochrony Lotniska i oznaczenia go odpowiednią klauzulą tajności;

- wyznaczenia stref zastrzeżonych i części krytycznych tych stref, a także wyznaczenia, w porozumieniu ze Strażą Graniczną i Policją, przejść ze strefy ogólnodostępnej do zastrzeżonej oraz zapewnienia ich ochrony (strefy zastrzeżone zarządzający lotniskiem określa w Programie Ochrony Lotniska).

Opracowany projekt Programu Ochrony Lotniska zarządzający przedstawia do uzgodnienia do Departamentu Ochrony i Uprawnień w Lotnictwie Cywilnym, a następnie do zatwierdzenia prezesowi Urzędu Lotnictwa Cywilnego. Zgodnie z art. 2. Ustawy z 1997 r. o ochronie osób i mienia plan ochrony powinien: uwzględniać rodzaj działalności jednostki, zawierać analizę stanu potencjalnych zagrożeń i aktualnego stanu bezpieczeństwa jednostki, podawać ocenę aktualnego stanu ochrony jednostki, zawierać dane dotyczące specjalistycznej uzbrojonej formacji ochronnej (w tym stan etatowy, rodzaj oraz liczbę uzbrojenia i wyposażenia, sposób zabezpieczenia broni i amunicji), zawierać dane dotyczące rodzaju zabezpieczeń technicznych, zasady organizacji i wykonywania ochrony jednostki.

Zaprojektowane systemy bezpieczeństwa służą do ochrony terminala lotniczego i składają się z systemów:

- kontroli dostępu (KD)
- sygnalizacji włamania (SSW)
- monitoringu wizyjnego (CCTV)
- kontroli wejścia i wnoszenia przedmiotów do obszaru bezpiecznego.

Systemy bezpieczeństwa są uzupełnieniem i współdziałają z zaprojektowanymi rozwiązaniami architektonicznymi wydzieleń stref. Systemy te powinny zostać uwzględnione w Planie Ochrony obiektu. Plan Ochrony powinien zawierać procedury stosowania i administrowania systemów technicznego zabezpieczenia.

System telewizji dozorowej

Zaprojektowano ochronę przestrzeni wspólnej: wejścia do budynku, poczekalnie, przejścia, wszystkie urządzenia bezpieczeństwa. Rozmieszenie kamer w projekcie wykonawczym na podstawie analizy bezpieczeństwa.

Do analizy, na potrzeby projektu, tam gdzie było to konieczne przywołano konkretny system: można użyć rozwiązania równoważnego. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

System telewizji dozorowej będzie funkcjonował i spełniał w całości postawione wymagania zawarte w normie PN-EN 50132-7:2003 Systemy alarmowe-Systemy dozorowe CCTV stosowane w zabezpieczeniach - część 7: Wytyczne stosowania. Zgodnie z normą "telewizja pracująca w obwodzie zamkniętym, w najprostszej postaci, jest narzędziem umożliwiającym obserwację na ekranie monitora obrazów z kamery telewizyjnej, dostarczonych za pośrednictwem prywatnej linii przesyłowej".

Procedura projektowania i instalacji systemu CCTV to:

1) opracowanie wymagań użytkowych,

2) zaprojektowanie systemu,

3) uzgodnienie wyboru urządzeń,

4. zainstalowanie i uruchomienie systemu,

5) przekazanie systemu klientowi,

6) utrzymanie w ruchu.

Głównym zadaniem systemu CCTV jest zwiększenie bezpieczeństwa.

Wymagania użytkowe:

a) określenie wymaganego poziomu zabezpieczenia(ocenę zagrożeń);

b) określenie obszaru lub przestrzeni objętej zasięgiem systemu;

c) wyjaśnienie celu objęcia zasięgiem systemu każdego obszaru lub przestrzeni;

d) określenie metody uzyskiwania informacji z obrazów telewizyjnych(ręcznie lub automatycznie);

e) określenie zadań, które mają być wykonane w następstwie obserwacji poszczególnych obrazów;

f) określenie przewidywanego czasu reakcji dla każdej części systemu;

g) określenie zakresu warunków otoczenia, w których system i jego elementy maja funkcjonować;
h) określenie gdzie, kiedy i przez kogo mają być wykonywane zadania(sterowanie);
i) określenie maksymalnej liczby jednoczesnych zdarzeń (w najmniej korzystnym przypadku), na które system powinien zareagować;
j) określenie wymagań dotyczących szkolenia;
k) listę wszystkich pozostałych czynników specjalnych, nie wymienionych wyżej.

Opis systemu monitoringu wizyjnego CCTV

Zaprojektowano system monitoringu wizyjnego oparty o cyfrowe przetwarzanie i cyfrowy zapis danych. Przesył sygnału wizyjnego kablem typu skrętka. Kamery zewnętrzne umieszczone w obudowach gwarantujących poprawne warunki środowiskowe pracy urządzeń.

Zaprojektowano kamery wewnątrz budynków: kolorowe stacjonarne i kopułkowe, kamery zewnętrzne stacjonarne zaprojektowano w obudowach przystosowanych do różnych warunków atmosferycznych. Wszystkie kamery będą posiadały obiektywy o zmiennej ogniskowej w celu precyzyjnego dopasowania obszaru obserwacji.

Głównym elementem systemu jest cyfrowy rejestrator obrazu.

Centrum obsługi systemu zaprojektowano pomieszczeniu 1.60 na poziomie +1.

Wszystkie kamery należy zamontować na systemowych uchwytach. Dla kamer zewnętrznych wysięg uchwytów powinien być jak największy. Uchwyty nadzy dobrać do rodzaju podłoża i lokalizacji kamery. Przewody należy prowadzić w uchwytach unikając prowadzenia na zewnątrz. Przy kamerach zewnętrznych należy zachować reżim montażu związany ze odpornością na warunki atmosferyczne i szczelność połączeń stosując odpowiednio dobrane dławiki do przewodów.

Zasilanie

Zasilanie wszystkich kamer będzie odbywać z najbliższych rozdzielni elektrycznych administracyjnych z wydzielonych obwodów zabezpieczonych bezpiecznikami nadmiarowymi.. Kamery zasilane prądem innym niż 230 V należy wyposażyć w zasilacze. Grzałki w kamerach zewnętrznych będą zasilane 230V bezpośrednio z rozdzielni elektrycznych przewodem YDY 3x1,5. Każdy tor zasilania musi posiadać zabezpieczenie przed przepięciem i zwarciem.

Ważniejsze wytyczne do systemu CCTV

- Projektowany system telewizji dozorowej CCTV realizowany będzie na kamerach IP,
- Rejestracja będzie odbywać się w trybie ciągłym w pełnej rozdzielczości kamer

– Okres przechowywania zapisu z kamer 30 dni – przy minimum 10kl/s w pełnej rozdzielczości kamer
– Serwery zostaną zlokalizowane w pomieszczeniu serwerowni 1.50 oznaczonej jako SOL na Poziomie +1
– Przewidywana ilość stanowisk podglądu 3.
– Dozorem wizyjnym powinny być objęte wszystkie punkty dozoru bezpieczeństwa: wyznaczone przejścia kontroli dostępu oraz wszystkie tzw. gate'y.
– Okablowanie strukturalne systemu telewizji dozorowej należy wykonać w kategorii 6A, dla kamer instalowanych na słupach kablem światłowodowym OM3.

Ogólna koncepcja systemu CCTV

Zastosowanie kamer systemu IP zapewni Użytkownikowi:
– Zbudowanie nowoczesnego i elastycznego systemu pozwalającego na łatwą rozbudowę o nowe punkty kamerowe w przyszłości
– prostą rozbudowę o dodatkowe stanowiska podglądu – nowe stanowiska mogą zostać podłączone do dedykowanej sieci w każdym, dowolnie wybranym pomieszczeniu, do którego zostanie doprowadzona dedykowana sieć strukturalna oraz zainstalowane oprogramowanie klienckie i przyznane przez Administratora systemu uprawnienia,
– łatwą zmianę lokalizacji poszczególnych kamer w przyszłości w razie potrzeby.
– łatwą zamianę punktów obserwacji lub także rejestracji,
– łatwą konfigurację oraz zmianę uprawnień do zarządzania systemem a także możliwości obserwacji rejestrowanych obrazów,
– zdecydowanie lepszą jakość obrazu i więcej szczegółów w obserwowanych scenach w porównaniu do systemów opartych na kamerach analogowych

Sieć strukturalna CCTV SOL

Dla projektowanego na obiekcie Systemu Telewizji Dozorowej wykonana zostanie dedykowana sieć strukturalna niezależna od ogólnej sieci komputerowej w budynku Terminala.
Sieć strukturalna ekranowana kat 6A zbudowana będzie w topologii gwiazdy z 2 Punktami Dystrybucyjnymi. Podział okablowania miedzianego na 2 strefy wynika z odległości do poszczególnych punktów montażu kamer i wymogu zachowania odległości nie większej niż 90m od Punktu Dystrybucyjnego do kamery. Poza kamerami stałopozycyjnymi zainstalowanymi w budynku terminala przewiduje się też montaż 6 kamer PTZ na słupach do obserwacji Terminala z

zewnątrz. Okablowanie kamer zewnętrznych zostanie wykonane kablem światłowodowym zakończonym w skrzynce słupowej. W Skrzynkach kabel światłowodowy zaterminować złączami SC i poprzez mediakonwertery przejść na kabel miedziany. Zasilacze kamer PTZ zainstalowane będą w skrzynkach słupowych do których musi byc doprowadzone zasilanie 230V.
Centrum systemu CCTV stanowić będzie serwerownia CCTV SOL usytuowana w pomieszczeniu 1.50 oznaczonej jako SOL na Poziomie +1. Tutaj zainstalowane zostaną Serwery wraz z oprogramowaniem do archiwizacji danych z monitoringu.
Punktami dystrybucyjnymi będą szafy 19" wyposażone w panele krosowe, switche, konwertery światłowodowe – tylko dla kamer PTZ zainstalowanych na zewnątrz budynku.
Połączenie pomiędzy PPD1 i PPD2 a GPD wykonane zostanie przy wykorzystaniu okablowania światłowodowego.
Zasilanie kamer za pomocą switchy z PoE, dla kamer PTZ zasilanie ze skrzynek słupowych poprzez dedykowane zasilacze.
Okablowanie sieci strukturalnej dla potrzeb telewizji dozorowej wykonane zostanie w kat.6A.
Podłączenie okablowania S/FTP do kamer będzie miało miejsce za pomocą patch cordów RJ-45 - RJ-45. Kable okablowania strukturalnego należy zakończyć w gniazdach podwójnych p/t z modułem RJ-45.
Punkty dystrybucyjne dla telewizji dozorowej montowane będą w tych samych pomieszczeniach co punkty dystrybucyjne ogólnej sieci komputerowej co zagwarantuje dużą elastyczność projektowanego systemu a także ułatwi jego ewentualną rozbudowę w przyszłości.
Do każdego punktu kamerowego prowadzić należy 2 kable logiczne. Przewidzieć ok. 5m zapasu kabla po stronie kamery. Kable będą prowadzone w trasach i korytkach kablowych okablowania strukturalnego.

Punkty dystrybucyjne CCTV SOL

Projektowane punkty dostępowe zostaną wykonane w oparciu o szafy 19" wys. min. 42U, szer. 800mm x gł. 800mm.
Każdy z Punktów dystrybucyjnych bedzie wyposażony w:

- Listwę zasilającą (wys. 1U),
- Panel światłowodowy (wys. 1U)
- Panele krosowe 24xRJ45 kat 6A
- Panele porządkujące (wys. 1U)
- 24 portowy switch z POE (wys. 1U),

Okablowanie miedziane z kamer zostanie wyprowadzone na Panele krosowe 24xRJ45 kat 6A. Następnie przy użyciu kabli krosowych (patchcordów) podłączone do Przełączników z PoE. Okablowanie światłowodowe kamer zewnętrznych prowadzone będzie w kanalizacji teletechnicznej i wprowadzone do budynku na przełącznicę.

Wymogi dla kamer

Kamery stałopozycyjne kopułowe montowane wewnątrz budynku

- kamery dzienno nocne (minimalne warunki oświetleniowe : 0.1 lx w kolorze i 0.07 lx w trybie czarno/białym)
- przetwornik 1/2.9-type progressive scan Exmor CMOS
- rozdzielczość FullHD 1920x1080 pikseli, 30kl/s, H.264 oraz JPEG
- obiektyw o zmiennej ogniskowej 3-9mm
- kąt widzenia w poziomie 105.2° deo 35.4°
- zoom cyfrowy 4x, zoom optyczny 3x
- stabilizacja obrazu
- zasilanie PoE (IEEE 802.3af compliant, Class 2).
- funkcja WDR
- redukcja szumów
- zdalna regulacja obiektywu - auto zoom i auto focus
- Równoczesna obsługa 3 strumieni video w różnych kombinacjach formatów kompresji H.264 lub JPEG.
- Możliwość wyboru w menu kamery różnych trybów obrazu, np: Standard, Priorytet poruszających się przedmiotów, Priorytet redukcji szumów.
- Inteligentna detekcja ruchu
-Funkcjonalność poprawy warunków oświetleniowych w jakich pracuje pozwalająca na wykonanie w krótkim czasie kilku ujęć tej samej sceny przy ustawieniach przesłony i ich nałożenie na siebie tak by dostarczać Użytkownikowi sceny bez zacienionych lub prześwietlonych obszarów.
- Analityka wbudowana w kamerę pozwalająca Użytkownikowi na definiowanie alarmowych w kamerze poprzez ustalenie reguł np: detekcja przekroczenia wirtualnej lini, zbyt długiego przebywania w danej strefie, wykrycie pozostawienia przedmiotu lub zniknięcie przedmiotu z pola obserwacji kamery
- Alarm antysabotażowy
- Możliwość ustawienia zmiennej (VBR) lub stałej szybkości bitowej (CBR) danych.

- Maski prywatności – pola wyłączone spod obserwacji kamery
- Kamera powinna obsługiwać następujące protokoły: IPv4, IPv6, TCP, UDP, ARP, ICMP, IGMP*, HTTP, HTTPS, SSL,SMTP, DHCP, DNS, NTP, RTP/RTCP, over TCP, RTSP over HTTP, and SNMP (v1, v2c, v3).
- Podstawowe zabezpieczenie dostępu do kamery poprzez hasło oraz filtrowanie adresów IP.
- Zakres temperatury pracy kamery (-10 ˚C do +50 ˚C)
- Zgodność z międzynarodowymi standardami ONVIF Profile umożliwiająca integrację kamery ze środowiskiem zewnętrznego oprogramowania i sprzętu.

Wandalodoporne kamery stałopozycyjne kopułowe

Wandalodoporne kamery stałopozycyjne kopułowe montowane w śluzach i przedsionkach
- kamera wandaloodporna (IK10) w wersji zewnętrznej IP66
- wbudowany doświetlacz o zmiennej mocy zapewniający możliwość obserwacji przy braku oświetlenia (0lx) do 30m.
- kamery dzienno nocne (minimalne warunki oświetleniowe : 0.1 lx w kolorze i w trybie czarno/białym przy włączonym doświetlaczu, 50 IRE)
- przetwornik 1/2.9-type progressive scan Exmor CMOS
- rozdzielczość FullHD 1920x1080 pikseli, 30kl/s, H.264 oraz JPEG
- obiektyw o zmiennej ogniskowej 3-9mm
- kąt widzenia w poziomie 105.2° deo 35.4°
- zoom cyfrowy 4x, zoom optyczny 3x
- zasilanie PoE/PoE+ (IEEE 802.3af compliant, Class 2, IEEE 802.3at).
- funkcja WDR
- redukcja szumów
- zdalna regulacja obiektywu - auto zoom i auto focus
- Równoczesna obsługa 3 strumieni video w różnych kombinacjach formatów kompresji H.264 lub JPEG.
- Możliwość wyboru w menu kamery różnych trybów obrazu, np: Standard, Priorytet poruszających się przedmiotów, Priorytet redukcji szumów.
- Inteligentna detekcja ruchu
-Funkcjonalność poprawy warunków oświetleniowych w jakich pracuje kamera pozwalająca na wykonanie w krótkim czasie kilku ujęć tej samej sceny przy różnych ustawieniach przesłony i ich nałożenie na siebie tak by dostarczać Użytkownikowi sceny bez zacienionych lub prześwietlonych obszarów.

- Analityka wbudowana w kamerę pozwalająca Użytkownikowi na definiowanie zdarzeń alarmowych w kamerze poprzez ustalenie reguł np: detekcja przekroczenia wirtualnej linii, zbyt długiego przebywania w danej strefie, wykrycie pozostawienia przedmiotu lub zniknięcie przedmiotu z pola obserwacji kamery
- Alarm antysabotażowy
- Możliwość ustawienia zmiennej (VBR) lub stałej szybkości bitowej (CBR) przesyłanych danych.
- Maski prywatności – pola wyłączone spod obserwacji kamery
- Kamera powinna obsługiwać następujące protokoły: IPv4, IPv6, TCP, UDP, ARPICMP, IGMP*, HTTP, HTTPS, SSL,SMTP, DHCP, DNS, NTP, RTP/RTCP, over TCP, RTSP over HTTP, i SNMP (v1, v2c, v3).
- Podstawowe zabezpieczenie dostępu do kamery poprzez hasło oraz filtrowanie adresów IP.
- Zakres temperatury pracy kamery (-10 ˚C do +50 ˚C)
- Zgodność z międzynarodowymi standardami ONVIF Profile umożliwiająca integrację kamery ze środowiskiem zewnętrznego oprogramowania i sprzętu.

Kamery PTZ montowane na słupach
- kamery dzienno nocne
- rozdzielczość FullHD 1920x1080 pikseli, 60kl/s, H.264 oraz JPEG
- zoom optyczny 30x
- wbudowany slot na karty pamięci SDHC
- zasilanie PoE+ (IEEE 802.3at)
- funkcja WDR
- redukcja szumów
- redukcja efektu mgły
- stabilizacja obrazu
- zdalna regulacja obiektywu - auto zoom i auto focus
- tryb automatycznych ustawień obrazu
- obsługa audio
- dodatkowe analogowe wyjście video
- Równoczesna obsługa strumieni video w różnych kombinacjach formatów kompresji H.264 lub JPEG.
- Analityka wbudowana w kamerę pozwalająca Użytkownikowi na definiowanie alarmowych w kamerze poprzez ustalenie reguł np: detekcja przekroczenia linii, zbyt długiego przebywania w

danej strefie, wykrycie pozostawienia przedmiotu lub zniknięcie przedmiotu z pola obserwacji kamery

- Możliwość ustawienia zmiennej (VBR) lub stałej szybkości bitowej (CBR) przesyłanych danych.
- Maski prywatności – pola wyłączone spod obserwacji kamery
- Kamera powinna obsługiwać następujące protokoły: IPv4, IPv6, TCP, UDP, ARP, ICMP, IGMP, HTTP, HTTPS, SSL,SMTP, DHCP, DNS, NTP, RTP/RTCP, RTSP over TCP, RTSP over HTTP, and SNMP (v1, v2c, v3).

- Podstawowe zabezpieczenie dostępu do kamery poprzez hasło oraz filtrowanie adresów IP.

- Zakres temperatury pracy kamery (-40 ˚C do +50 ˚C)

- Zgodność z międzynarodowymi standardami ONVIF Profile umożliwiająca integrację kamery ze środowiskiem zewnętrznego oprogramowania i sprzętu.

Wymogi dla systemu VMS

System Zarządzania wideo ma być oparty na protokole TCP/IP i umożliwiać Zamawiającemu zbudowanie własnego systemu nadzoru wideo z z wykorzystaniem standardu wideo i sprzętu komputerowego. Ze względu na charakter planowanej inwestycji System zarządzania obrazem powinien być bardzo wydajny i mieć możliwość rozbudowy o aplikacje analityki wideo oraz integracji z innymi aplikacjami biznesowymi w każdym środowisku IT. System zarządzania obrazem powininen być dedykowany dla dużych wdrożeń o wielu lokalizacjach, gdzie scentralizowane zarządzanie jest kluczowym wymogiem. System powinien mieć możliwość nieograniczonego zwiększania ilości kamer, użytkowników i lokalizacji

- System Zarządzania wideo (VMS) powinien składać się min. z następujących elementów:
    - Serwer zarządzający (Management server)
    - Serwer zapisu (Recording server)
    - Serwer zdarzeń (Event server)
    - Klient zarządzający (Management Client)
    - Aplikacja kliencka (Smart Client)
    - Zdalna przeglądarka kliencka
    - Aplikacja kliencka dla urządzeń mobilnych
- System zarządzania obrazem powinien być rozwiązaniem które może być rozproszone w wielu miejscach i na wielu serwerach, dla instalacji wymagających nadzoru 24/7 z obsługą urządzeń

pochodzących od różnych dostawców. Federacyjna architektura systemu umożliwia nieograniczone skalowanie, elastyczność i dostępność

- System zarządzania obrazem powinien zapewniać centralne zarządzanie wszystkimi urządzeniami, serwerami i użytkownikami.
- System zarządzania obrazem powinien zawierać serwery rejestrujące używane dla kanałów nagrywania wideo i do komunikacji z kamerami i innymi urządzeniami. Serwery rejestrujące powinny obsługiwać proces nagrywania i odtwarzania strumieni wideo.
- System zarządzania obrazem powinien zawierać serwer zarządzający, który będzie centralnym menedżerem systemu i będzie pełnił funkcje kontrolne wobec serwerów rejestracji, kamer, urządzeń oraz użytkowników. Serwer zarządzający powinien sprawować nadzór nad logowaniem się klienta i konfiguracji systemu.
- System powinien obsługiwać funkcjonalność Multi cast- wysyłać tylko jeden strumień danych z kamery do wielu Klientów
- System powinien automatycznie wykrywać nowe urządzenia IP - kamery, enkodery oraz rejestratory pochodzące od różnych producentów.
- Funkcja Eksploratora Sekwencji – Wyświetla sekwencje, odstępy czasowe i znaczniki zdarzeń zapewniająca unikalny przegląd nagranego materiału połączony z łatwą nawigacją.
- 64 bitowy Serwer zapisu pozwalający na podłączenie większej ilości kamer do jednego serwera
- Elastyczność zarządzania profilem Użytkownika i uprawnieniami Ograniczanie uprawnień Klientów do określonych funkcji i ustawień kamery. Modularność zarządzania profilami Klientów od podstawowych do globalnych.
- Maski prywatności- możliwość określenia stref prywatności dla indywidualnych kamer i zaznaczenia obszarów wyłączonych spod obserwacji i rejestracji obrazu.
- System Monitor –funkcjonalność dostarczająca dane o aktualnej i historycznej wydajności systemu, parametrach pracy serwera, dostępności powierzchni dyskowej, obciążeniu sieci i parametrów pracy kamery.
- Nielimitowana ilość kamer, lokalizacji, serwerów oraz Użytkowników zapewniająca nieograniczoną elastyczność w rozbudowie systemu.
- Scentralizowane zarządzanie systemem: Pełna konfiguracja wszystkich urządzeń, Recording serwerów, Użytkowników z poziomu konsoli centralnego menedżera podłączonej do Serwera zarządzania przechowującego wszystkie ustawienia w bazie Microsoft SQL
- Etykietowanie - pozwalające Użytkownikowi oznaczać i dodawać opisy do konkretnych partii materiału video przeznaczonego do dalszej analizy lub przekazania innym Użytkownikom ze względu na wskazane parametry

- Alarm Manager - funkcjonalność zapewniająca wgląd do zdarzeń alarmowych w systemie dozoru wizyjnego i powiązanych systemach bezpieczeństwa.
- Intuicyjna wielowarstwowa mapa. Wielowarstwowe środowisko map zapewniające interaktywny dostęp i kontrolę nad systemem dozoru wizyjnego,
- Funkcja Edge Storage wykorzystująca pamięć wbudowaną w kamerze jako komplementarną do centralnego zapisu. Pozwala na elastyczność wydobywania danych według wskazanych harmonogramów, zdarzeń lub zleceń ręcznych.
- Wielostopniowe archiwum pozwalające na powiązanie wysokiej wydajności i skalowalności z przygotowaniem danych video do długotrwałego ekonomicznego przechowywania.
- Wszechstronny system reguł zapewniający łatwość automatyzacji różnych aspektów pracy systemu włącznie z kontrolą kamer, zachowaniem systemu oraz urządzeń zewnętrznych typu oświetlenie, drzwi na podstawie zdarzeń lub rozkładów czasu. Funkcjonalność pozwala na eliminację manualnej kontroli.
- Funkcja Szybkiego eksportu materiału dowodowego- przesył danych do organów ścigania lub administracji publicznej wraz z aplikacją do ich odtworzenia
- System zarządzania obrazem powinien zawierać moduł danych umożliwiający integrację z wieloma aplikacjami analityki video (VCA) dostarczanymi przez innych dostawców
- System zarządzania obrazem powinien zawierać Software Development Kit (SDK), który zapewni możliwość integracji tego systemu z aplikacjami innych dostawców.
- System zarządzania obrazem powinien zapewniać wsparcie dla Active Directory, aby umożliwić łatwe dodawanie użytkowników do systemu. Korzystanie z Active Directory wymaga, aby serwer z systemem Active Directory, działający jako kontroler domeny, był dostępny w sieci.
- Funkcja Multi-live streaming pozwalająca na definiowanie wielu strumieni danych o różnych parametrach do podglądu na żywo.
- Równoległe nagrywanie wielu strumieni danych z kamer i enkoderów IP w formatach MJPEG, MPEG-4, MPEG4-ASP, MxPEG, H.264 bez ograniczeń co do ilości kamer na serwer.
- Dwukierunkowe audio, transmisja i nagrywanie sygnału audio z zainstalowanych mikrofonów oraz z mikrofonu operatora do zainstalowanych głośników.
- Przekazywanie obrazu na żywo z kamer do wielu Klientów równocześnie, odtwarzanie oraz eksport materiału.
- Dedykowany strumień nagrywania pozwala na optymalizację rozdzielczości, poklatkowości, kodeków na potrzeby przechowywania i przyszłego zastosowania.
- Bezpieczna baza szybkiego nagrywania materiału video w formatach JPEG, MPEG4, MPEG4-ASP, lub H.264

- Nagrywania z prędkości przekraczającą 30 kl/s na kamerę, uzależnione od możliwości samej kamery.
- Brak ograniczeń programowych dla jakości nagrywanego materiału
- Możliwość importu obrazu z pamięci pre-alarmowej kamery
- Wbudowany, niezależny od kamery system detekcji ruchu w czasie rzeczywistym
- Obsługa adresacji IPv4 oraz IPv6
- Cyfrowy opis rejestrowanego materiału video do weryfikacji czy nie był poddawany modyfikacji po wyeksportowaniu lub podczas przechowywania
- Usługa zdalnego łączenia zapewniająca bezpieczeństwo zdalnego podłączania do systemu kamer za pośrednictwem sieci prywatnych lub publicznych
- Pierwszeństwo kontroli ręcznej PTZ dla uprzywilejowanych Klientów
- 32000 poziomów priorytetów PTZ dla kontroli uprawnień między operatorami oraz zaprogramowanymi trasami patrolowania
- Określenie regułami ustawień kamery wywołanych wskazanymi zdarzeniami alarmowymi lub trasami patrolowania.
- Przerwanie trasy patrolowej przez zdarzenie alarmowe i ponowny powrót urządzenia do zadanej trasy
- Wsparcie dla urządzeń posiadających jedno lub więcej wejść alarmowych
-Serwer nagrywania jest całkowicie zarządzany z poziomu Serwera zarządzającego, wszelkie zmiany konfiguracji są możliwe natychmiastowo w trakcie nagrywania
- Dostęp do konfiguracji lokalnego Serwera zapisu podczas gdy Serwer zarządzający jest niedostępny
- Serwer nagrywania dostępny w lokalnej strefie powiadomień konsoli dla informacji o statusie, zatrzymaniu/uruchomieniu usług oraz zmian ustawień sieciowych.
- Klienci są identyfikowani i autoryzowani przez Serwer zarządzający i korzystają z ograniczonego sesyjnie tokenu do dostępu do Serwera zapisu
- System pracuje jako agent SNMP i może generować komunikaty Trap
- Definiowanie jednego lub więcej miejsc zapisu z indywidualnie określanymi schematami i okresem przechowywania. Pojemność nagrań ograniczona jest tylko powierzchnią dysków.
- Reguły archiwizacji określające kiedy materiał jest przekazywany do kolejnego poziomu przechowywania i jak długo pozostaje w bazie do momentu zniszczenia.

7 .Urządzenia aktywne.

W celu zapewnienia niezawodności projektowanego rozwiązania jak i optymalnego wykorzystania zasobów sieciowych przewiduje się zastosowanie technologii wieżowania i agregacji połączeń sieciowych /LACP/.
Przełączniki PoE 24 portowe w Punktach Dystrybucyjnych zostaną zestakowane i podłączone kablami światłowodowymi przy użyciu modułów SFP do rdzenia systemu - Przełączników głównych pracujący również w oparciu o technologię wieżowania.
Każdy z 3 serwerów zapisu posiada po 4 porty LAN 1GB i będzie podłączony do obu przełączników rdzeniowych systemu CCTV w Serwerowni.

Punkt rejestracji

Sygnały z kamer przesłane będą za pomocą kabli miedzianych do punktów dystrybucyjnych, skąd za pośrednictwem urządzeń aktywnych zostaną doprowadzone do serwera zapisu systemu w pomieszczeniu Serwerowni. Zapis danych będzie odbywał się na serwerach zamontowanych w dedykowanej dla systemu CCTV szafie dystrybucyjnej o wysokości min. 42U.
Przewidziano montaż serwerów dedykowanych do monitoringu wizyjnego IP, zoptymalizowanych pod kątem zastosowanych elementów dostarczonych przez renomowanych productenów IT.
Serwery oparte o technologię 6G SAS przewyższające zdecydowanie parametrami technicznymi serwery z dyskami SATA, pozwalające na równoczesny odczyt i zapis danych na dyskach.
Serwery pracują w trybie FullDuplex i 2 aktywne kanały przesyłu danych. Procesor Intel Xeon E5-2420 z zegarem 1.9GHZ 6C, porty LAN 4x1GB. Montaż rack, 2U.
Rejestracja danych z monitoringu bedzie odbywać się na 2 Serwerach 2U o pojemności całkowitej 16TB każdy i dołączonych do nich pamięci masowych DAS 24TB.
Oprogramowanie zarządzające zostanie zainstalowane na dedykowanym serwerze 1U.

Stanowiska obserwacji i analizy obrazu.

Do obserwacji zdarzeń z kamer konieczne będą tzw. stanowiska obserwacyjne. Będą to specjalnie skonfigurowane komputery ze oprogramowaniem klienckim oraz w zależności od rodzaju stanowiska rodzajem przydzielonych uprawnień.
Struktura systemu zastała tak pomyślana, aby stanowiska podglądu mogły być instalowane w dowolnym wybranym przez Użytkownika pomieszczeniu, do którego doprowadzona będzie sieć systemu CCTV. Podłączenie sieci sprowadza się do doprowadzenia okablowania wpiętego do switcha w punkcie dystrybucyjnym. Administrator systemu może ustanowić użytkowników o dostępie dla różnych kamer z różnym stopniem uprawnień: od samej obserwacji obrazów z kamer

na żywo, poprzez regulacje kamerami obrotowymi, aż po przeglądanie, kopiowanie i usuwanie archiwum.

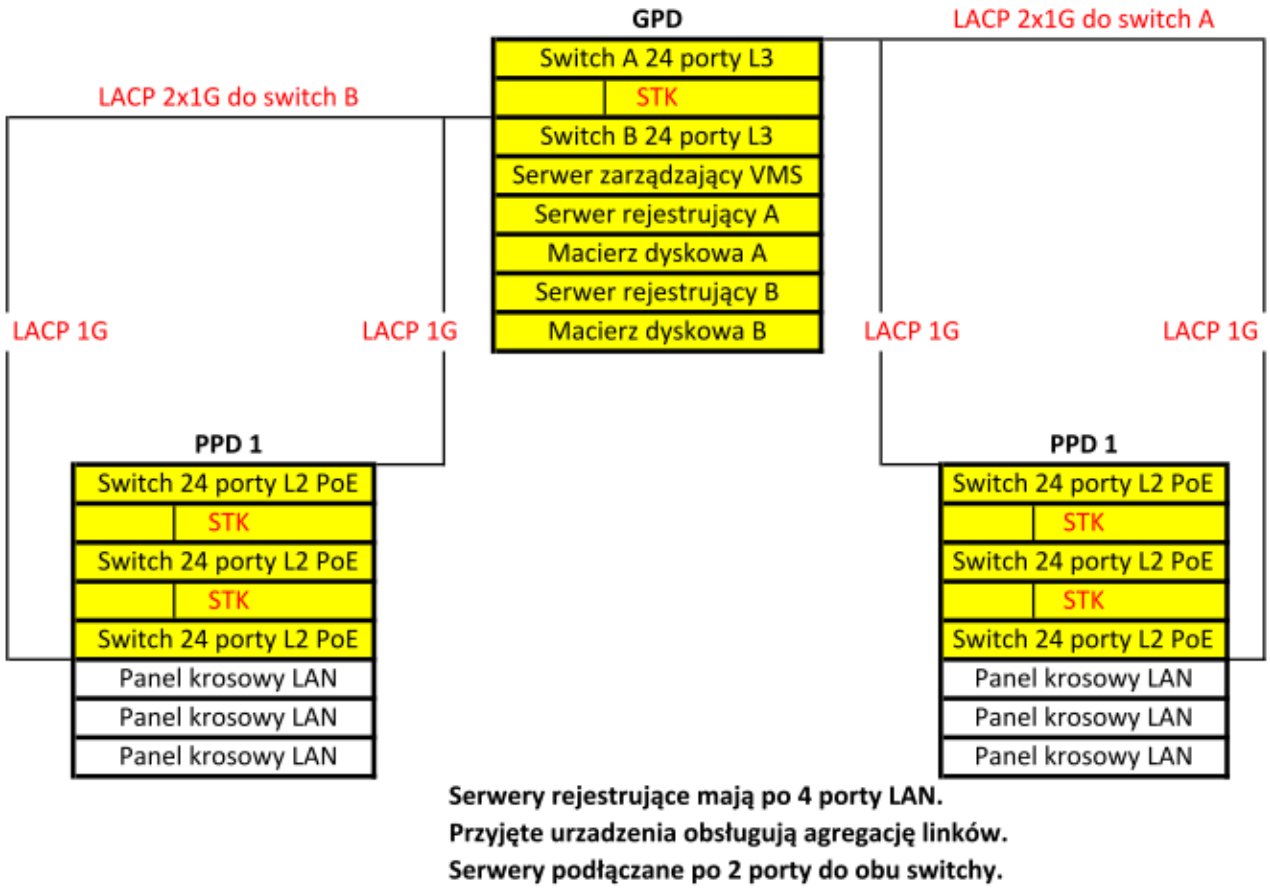
W skład stanowiska podglądu wchodzić będzie:

– Dedykowana stacja robocza PC, z procesoerem 3.6GHz -
– System operacyjny 64BIT-
– Karta graficzna z 2 wyjściami ,
– 2 monitory 42”,
– pulpit sterujący kamerami obrotowymi

Miejsca montażu stanowisk podglądu, rodzaje uprawnień i dostęp do obserwowanych kamer a także zapisywanych danych, Użytkownik systemu przyzna dopiero na etapie odbioru systemu, korygując je w trakcie użytkowania. Przewiduje się montaż 3 stanowisk podglądu. Głównym stanowiskiem podglądu będzie zlokalizowane w pomieszczeniu SOL .

Schemat funkcjonalny systemu

Poniżej został przedstawiony schemat funkcjonalny budowy części transmisyjnej i serwerowej systemu monitoringu wizyjnego.



Zestawienie materiałów

Do analizy, na potrzeby projektu, tam gdzie było to konieczne przywołano konkretny system: można użyć rozwiązania równoważnego. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

PN	Opis Kamery	Ilość	jm
SNC- EM632R	Kamera IP kopułkowa, zewnętrzna, wandaloodporna, z doświetlaczem IR, przetwornik 1/2.9-type progressive scan Exmor CMOS sensor, Full HD , czułość Color: 0.1 lx (F1.2, View-DR OFF, VE OFF, AGC ON, 1/30 s, 30 fps), B/W: 0 lx, obiektyw zmienno-ogniskowy f = 3.0 mm to 9.0 mm, kąt widzenia 105.2° to 35.4°, slot na karty SDHC, IK10, IP66, ONVIF, zasilanie DC 12V, AC 24V, PoE+. Easy focus, Analityka -DEPA	7	szt.
SNC-EM630	Kamera IP kopułkowa, przetwornik 1/2.9-type progressive scan Exmor CMOS sensor, Full HD, czułość Color: 0.1 lx (F1.2, View-DR OFF, VE OFF, AGC ON, 1/30 s, 30 fps), B/W: 0 lx, obiektyw zmienno-ogniskowy f = 3.0 mm to 9.0 mm, kąt widzenia 105.2° to 35.4°, slot na karty SDHC, ONVIF, zasilanie DC 12V, AC 24V, PoE. WDR, Easy zoom, Easy focus, Analityka- DEPA.	108	szt.
SNC-WR632	Kamera IP PTZ, Full HD, zoom optyczny x30, ONVIF, WDR, Redukcja szumów XDNR, Analityka -DEPA, Visibility enhancer, tryb redukcji mgły, stabilizacja obrazu, inteligentna detekcja twarzy i obiektów, 60kl/s, obrót w poziomie 700°/s.	6	szt.
	Akcesoria montażowe	6	kpl.
	Zasilacz kamery PTZ zewnętrzny	6	szt.
RM-NS1000	USB Joystick remote control unit	3	szt.
FWD-42B2	Flat Wide Display 42", LED backlight, 500cd/m2	6	szt.

PN	Opis Urządzenia aktywne	Ilość	
AT-x610-24Ts-60	Przełącznik Allied Telesis AT-x610-24Ts-60 20 portów 10/100/1000T + 4porty combo. Wysokowydajny i skalowalny przełącznik warstwy 3/3+ .	3	szt.
AT-8000GS/24POE-50	Przełacznik warstwy 2 Allied Telesis serii 8000GS 24x10/100/100T + 4xSFP. Wsparcie PoE (802.3af).	6	szt.
AT-SPSX	1G SFP Pluggable Optical Modules and Direct Attach cables	8	szt.
AT-STACKXG-00	Moduł stakujacy	2	szt.
PN	Opis Serwery i stacje robocze	Ilość	
BCD420V-CWP-2D-1G	Dedykowana stacja podglądu CCTV IP serii Z420 E5-1620 3.6GHz - System operacyjny WIN 7 64BIT- Karta graficzna z 2 wyjściami - gwarancja NBD on-site.	3	kpl.
BCD360V8-M-VMS	Dedykowany serwer zarządzający systemem CCTV IP DL360E (1)E5-2420 1.9GHZ- SERVER 2008 R2- gwarancja NBD on-site.	1	kpl.
BCD380V8-M-O4LA-16TB-2	Dedykowany serwer rejestrujący CCTV IP DL380E o pojemności całkowitej 16TB Procesor Intel Xeon E5-2420 1.9GHZ 6C. Technologia 6G SAS, porty LAN 4x1G-2420 1.9GHZ- SERVER 2008 R2- gwarancja NBD on-site.	2	kpl.
BCD2600V-24TB-2	24TB DIRECT ATTACHED STORAGE	2	kpl.
BCD380V8-EXT-RAID-CONTL	BCDVideo - EXTERNAL RAID CONTROLLER	2	kpl.
PN	Opis System VMS	Ilość	
XPETBL	XProtectExpert Licencja bazowa	1	szt.
XPETDL	XProtectExpert Licencja kamera/inne urządzenie	121	szt.
YXPETBL	SUP- 1 rok, licencja bazowa	1	szt.
YXPETDL	Sup- 1 rok, licencja kamerowa	121	szt.

Do analizy, na potrzeby projektu, tam gdzie było to konieczne przywołano konkretny system: można użyć rozwiązania równoważnego. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Kontrola dostępu i system sygnalizacji włamania

Opis systemu

Do analizy, na potrzeby projektu, tam gdzie było to konieczne przywołano konkretny system: można użyć rozwiązania równoważnego. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.
Zaprojektowano kontrolę dostępu we wszystkich przejęciach między strefami o różnych funkcjach i różnym stopniu bezpieczeństwa. Dodatkowo kontrolą dostępu objęto wejścia do pomieszczeń związanych z obsługą portu lotniczego. Kontrolą dostępu i systemem sygnalizacji włamania zabezpieczono węzły sieci i serwerownie.
Do drzwi z kontrolą dostępu zaprojektowane zamki elektromotoryczne rewersyjne (otwarcie w przypadku zaniku napięcia). Każde drzwi zaopatrzone w kontrolę dostępu wyposażone są w styk kontrolujące drzwi informujący o nieuprawnionym otwarciu (wyłamaniu) skrzydła. Zamek elektromotoryczny zapewnia skuteczne zamknięcie przejścia, obsługuje funkcję wyjścia ewakuacyjnego. Dla drzwi na przejściach ewakuacyjnych przewidziano przyciski wyjścia awaryjnego działające bezpośrednio poprzez odcięcie napięcia zasilającego zamek i powodując możliwość otwarcia drzwi klamką. System sprawdza położenie rygla zamka, stan zasprzęglenia klamki oraz monitoruje okablowanie. Dodatkowo, w przypadku wystąpienia pożaru system sygnalizacji pożaru może wysterować otwarciem drzwi zaopatrzonych w kontrolę dostępu programowo. Funkcja ta jest funkcja dodatkową nie mogącą zastąpić funkcji ewakuacji realizowanej twardo drutowo. Algorytm otwarcie drzwi i decyzje które przejście i w jakim momencie mają zostać otwarte zależy od Planu Ochrony obiektu. Drzwu rozsuwane sterowane są z KD w sposób: KD odblokowuje możliwość otwarcia drzwi przez automat dzrwiowy.
Zaprojektowana klawiatura systemu sygnalizacji włamania jest w pomieszczeniu 1.60 przy stanowisku Dyżurnego SOL oraz w pomieszczeniu 0.14 Operator SOL. Wejście do pomieszczeń strzeżonych systemem sygnalizacji włamania wymaga więc zgody Dyżurnego SOL. Organizacja taka ma zapobiegać nieuprawnionemu manipulowaniu przy węzłach sieci strukturalnej.
Na schemacie systemu pokazano organizację połączeń wszystkich urządzeń kontroli dostępu oraz systemu sygnalizacji włamania.
Sygnalizacja włamania została zaprojektowana w węzłach sieci i w kasie. Wykorzystane są czujki dualne (PIR i mikrofala) z antymaskingiem i antysabotażem. Dwie syreny alarmowe do

powiadomienia obsługi w pomieszczeniu dyżurnego portu oraz na korytarzu w okolicach pomieszczeń SOL, SG i SC.
System kontroli dostępu będzie wykorzystywany jako element systemu przepustek. Właściwe procedury wydawania przepustek, łączenia kart KD z przewodnikiem, zakres dostępu dla osoby posiadające przepustkę opisane w Planie Ochrony obiektu będą mogły być zaimplementowane w systemie KD.
Na stanowisku wydawania przepustek zaprojektowano stację operatora KD z oprogramowaniem wizualizacyjno - sterujące oraz programator kart KD.

Zestawienie przejść wyposażonych w kontrolę dostępu

lp	nr pomieszczenia	opis pomieszczenia	opis przejścia	przejścia	czytnik	zamek
1	0. 19	strefa VIP	wyjście na zewnątrz	1	2	1
2	0. 17	pomieszczenie odlotów	wejście	1	1	1
3	0. 16	briefing/meteo	wejście	1	1	1
4	0. 14	pom. Kontroli	wejście	1	1	1
5	0. 15	kontrola bezpieczeństwa	przejście do/z 0.1 hala strefa ogólnodostępna	1	2	1
6	0. 13	pom. wod. kan.	wejście	1	1	1
7	0. 11	klatka schodowa	przejście do/z 0.12 komunikacja	1	2	1
8	0. 11	klatka schodowa	wyjście na zewnątrz	1	2	1
9	0. 43	SG	wejście	1	1	1
10	0. 32	SG	wejście	1	1	1
11	0. 31	pom. przeszukań	wejście	1	1	1
12	0. 30	S.C.	wejście	1	1	1
13	0. 1	hala strefa ogólnodostępna	przejście do/z 0.29 strefa przylotów Schoengen	drzwi rozsuwane	2	
14	0. 1	hala strefa ogólnodostępna	przejście do/z 0.29 strefa przylotów Schoengen	drzwi rozsuwane	2	
15	0. 51	bagaż zagubiony	wejście	1	1	1
16	0. 25	śluza	wejście z 0.27 strefa przylotów	1	2	1

lp	nr pomieszczenia	opis pomieszczenia	opis przejścia	przejścia	czytnik	zamek
17	0. 27	strefa przylotów non Schoengen	wyjście na zewnątrz drzwi rozsuwane podwójne	1	2	
18	0. 29	strefa przylotów Schonegen	wyjście na zewnątrz drzwi rozsuwane podwójne	1	2	
19	55A	pom.mag.tech	wejście	1	1	1
20	0. 62	kontrola bagażu	wejście	1	1	1
21	0. 61	rozładunek / załadunek wózków	wyjście na zewnątrz drzwi rozsuwane jednokierunkowe	1	1	
22	0. 61	rozładunek / załadunek wózków	wejście od zewnątrz drzwi rozsuwane jednokierunkowe	1	1	
23	0. 63	pom. elektr.	wejście	1	1	1
24	0. 68	pom. dla obsługi handingowej	wejście	1	1	1
25	0. 69	komunikacja	wyjście na zewnątrz	1	2	1
26	0. 60	pom. Kontroli bagażu	wejście	1	1	1
27	0. 66	komunikacja	przejście do/z 0.59 sortowania bagażu	1	2	1
28	0. 76	kontrola bezpieczeństwa pracowników	przejście do/z 0.01 hala strefa ogólnodostępna	1	2	1
29	0. 77	pom. Kontroli broni	wejście	1	1	1
30	0. 79	SG	przejście do/z 0.01 hala strefa ogólnodostępna	1	2	1

lp	nr pomieszczenia	opis pomieszczenia	opis przejścia	przejścia	czytnik	zamek
31	0. 79	SG	przejście do/z 0.80 kontrola bezpieczeństwa	1	2	1
32	0. 83	SOL	wejście	1	1	1
33	0. 84	pom. przeszukań	wejście	1	1	1
34	0. 85	SG kasa	wejście	1	1	1
35	0. 1	hala strefa ogólnodostępna	przejście do/z 0.80 kontrola bezpieczeństwa	drzwi rozsuwane	2	
36	0. 86	korytarz do WC personelu	wejście	1	1	1
37	0. 108	kontrola paszportowa	wejście	1	1	1
38	0. 107	hala odlotów non Schoengen	wyjście na zew. drzwi rozs. podwójne	1	2	
39	0. 109	hala odlotów Schoengen	wyjście na zewnątrz drzwi rozsuwane podwójne	1	2	
40	0. 91	S.C.	wejście	1	1	1
41	0. 114	komunikacja	przejście do/z 0.01 hala strefa ogólnodostępna	1	2	1
42	0. 114	komunikacja	przejście do/z 0.120 klatka schodowa	1	2	1
43	0. 120	klatka schodowa	wyjście na zewnątrz	1	2	1
44	1. 3	pom.techn	wejście	1	1	1
45	1. 4	komunikacja	przejście do/z 1.2 komunikacja	1	2	1
46	1. 4	komunikacja	przejście do/z 1.1 schody	1	2	1

lp	nr pomieszczenia	opis pomieszczenia	opis przejścia	przejścia	czytnik	zamek
47	1. 17	taras bwidokowy	przejście do/z 1.4 komunikacja	1	2	1
48	1. 37	korytarz	przejście do/z 1.29 taras widokowy	1	2	1
49	1. 38	pom.adm. SC	wejście	1	1	1
50	1. 39	pom.adm. SC	wejście	1	1	1
51	1. 41	pom.adm. SOL	wejście	1	1	1
52	1. 42	pom.socjalne	wejście	1	1	1
53	1. 48	pom.adm. SG	wejście	1	1	1
54	1. 49	pom.adm.SG	wejście	1	1	1
55	1. 50	serwerownia SOL	wejście	1	2	1
56	1. 51	serwerownia SG	wejście	1	2	1
57	1. 52	serwerownia SC	wejście	1	2	1
58	1. 53	serwerownia zarz.lot.	wejście	1	2	1
59	1. 54	przedsionek	przejście do/z 1.37 korytarz	1	2	1
60	1. 55	pom.techn. DSO	wejście	1	1	1
61	1. 60	pom.centrum	przejście do/z 1.54 przedsionek	1	2	1
62	1. 61	pom.biurowe	wejście	1	1	1
63	1. 63	po.techn.	wejście	1	1	1
64	1. 64	klatka schodowa	przejście do/z 1.37 korytarz	1	2	1

Elementy systemu

Poniżej opisano analizowane w projekcie rozwiązanie budowy systemu. Można, przy zachowaniu nie gorszych parametrów technicznych opisanych w projekcie i parametrów funkcjonalnych opisanych w projekcie użyć innych niż zaprojektowanych elementów. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Centrala alarmowa systemu kontroli dostępu

Do analizy w projekcie przyjęto centralę alarmową Advisor MASTER.

Cechy central alarmowych systemu ATS:

Zasilacz – centrale są wyposażone w ten sam układ zasilacza impulsowego o wydajności 2,2A@13,8VDC (3.5A dla ATS4604N) przystosowanego do pracy buforowej.

Dialer – Standardowym wyposażeniem centrali jest komunikator telefoniczny przystosowany do komunikacji ze stacjami monitorującymi jak również do połączeń modemowych z komputerem. Prędkość transmisji jest ograniczona.

Magistrala MI – Centrale można rozbudować o potrzebne urządzenia komunikacyjne dzięki magistrali MI. Dostępne moduły umożliwiają komunikację ze stacjami SMA przez sieć GSM, ISDN oraz raportowanie głosowe

Połączenie serwisowe – centrala jest wyposażona w złącze RS232 pozwalające na komunikację serwisową z programem konfiguracyjnym (TITAN).

Zegar systemowy – Jednostka centralna jest wyposażona w autonomiczny układ czasu rzeczywistego RTC synchronizowanego generatorem kwarcowym. Zapewnia to dokładny pomiar czasu niezależny od obciążenia procesora, częstotliwości sieci energetycznej czy innych zjawisk środowiskowych. Korekta systematyczna czasu może być wprowadzona programowo jako wielkość –119 do 119 sekund/dzień.

Linie dozorowe – Wszystkie wejścia systemowe są przetwarzane przez konwerter A/C, a następnie poddawane analizie stanu wejścia przez procesor w centrali lub MZD. Na płycie centrali znajduje się 8 lub 16 linii dozorowych. Ich liczba może być zwiększona przez zastosowanie rozszerzenia ATS1202.

Rezystory końca linii – System może współpracować z trzema różnymi wielkościami rezystora końca linii (EOL): 2k2, 4k7 lub 10k. Domyślnie wykorzystywany jest 4k7Ohm.

Sygnalizatory – Każda centrala posiada 3 wysoko-prądowe, monitorowane wyjścia sygnalizatorów do podłączenia syreny zewnętrznej, wewnętrznej i lampy.
Pamięć – Wbudowana pamięć centrali wystarczy do obsługi typowego systemu alarmowego o niewielkim stopniu komplikacji (50 użytkowników, 250 zdarzeń, 10 grup alarmowych).
Pamięć centrali można rozszerzać stosując odpowiednie moduły.
Magistrala – Magistrala systemowa (RS485) pozwala na podłączanie manipulatorów, rozszerzeń alarmowych i kontroli dostępu. Ten sam interfejs jest stosowany do łączenia central w sieć oraz do magistral lokalnych niektórych urządzeń.
Rozszerzenia:
Magistrala MI – Komunikatory ISDN, GSM oraz moduł raportowania głosowego.
Interfejs drukarki i komputera – pozwala na podłączenie centrali na stałe do komputera, łączenie central w sieć oraz do łączenia centrali do systemu zdalnego w celu zarządzania czy serwisu.
Linie dozorowe – Linie dostępne na płycie centrali mogą być rozszerzane przy użyciu ATS1202 do 32 linii alarmowych. Pozostałe linie z limitu objętości centrali dostępne są w rozszerzeniach MZD podłączanych do magistrali systemowej.
Wyjścia systemowe – Na złączu w centrali dostępne są 4- wyjścia typu ‘OC’. Podłączając do złącza synchroniczne karty rozszerzeń (ATS1811/20) można powiększyć liczbę dostępnych wyjść do 128 wyjść przekaźnikowych lub 256 wyjść typu ‘OC’ – ograniczeniami są: maksymalna ilość modułów rozszerzeń, ilość miejsca na rozszerzenia w obudowie oraz dostępność zasilania. Dodatkowo centrale wyposażone są w wyjście przekaźnikowe NC/NO.
Magistrala – Pozwala podłączyć 16 manipulatorów (stacji ZAZ) oraz 15 ekspanderów (modułów MZD) pozwalających na wykorzystanie wszystkich linii alarmowych oraz dodatkowych funkcji kontroli dostępu – sterowniki drzwi i wind.
Centrala Alarmowa posiada 16 stacji ZAZ, z których każda może służyć do jednostronnego sterowania drzwiami. Każda stacja ZAZ jest wyposażona w wejście do podłączenia przycisku wyjścia oraz wyjściem do sterowania pracą rygla lub zamka elektromagnetycznego.
Obciążalność tych wyjść jest ograniczona do 50mA, dlatego należy stosować dodatkowe urządzenia sterujące urządzeniami wykonawczymi. W tym celu zaleca się stosowanie skrzynki połączeniowej ATS1340, która zawiera odpowiednie połączenia dla magistrali systemowej, zasilania, stacji ZAZ, przycisku wyjścia, oraz urządzeń wykonawczych. Centrala alarmowa nie jest przystosowana do zasilania urządzeń wykonawczych (zamków elektromagnetycznych, rygli, itp.), dlatego w fazie projektowania należy uwzględnić odpowiednie zasilanie dla tych urządzeń.
Drzwi obsługiwane przez stacje ZAZ mogą być monitorowane w sposób ciągły przez system alarmowy dzięki opcjom programowym zawieszania linii nadzorującej stan drzwi. System kontroli

dostępu wykorzystuje te same kody PIN oraz te same urządzenia, co cześć alarmowa. Jednocześnie urządzenia kontroli dostępu mogą być wykorzystywane do sterowania systemem alarmowym. Dotyczy to w szczególności czytników kart, które dzięki funkcjom zliczania użyć karty mogą zmieniać swoje działanie np.: potrójne użyciem karty użytkownik może zazbroić system wychodząc.

Płyta główna ATS4018 dane techniczne:
16 linii dozorowych na płycie
Maksymalne rozszerzenie do 32 linii;
256 linii w systemie
16 niezależnych obszarów
138 Grupy Alarmowe
120 Grupy Drzwi
11k-67k użytkowników
1000 Zdarzeń alarmowych
1000 Zdarzeń kontroli dostępu
Obudowa typu L – ATS1642
Sterowane wyjście zasilania
Rozszerzenia:
Pamięć
Interfejs komputera i/lub drukarki
Komunikacja
Wejścia/Wyjścia

Centrala ATS4618 posiada płytę główną ATS4018 wyposażoną w podstawowe rozszerzenie pamięci ATS1830 1Mb i obudowę typu L. Płyta główna centrali jest dostarczana z obudową typu L – ATS1642 oraz zasilaczem o wydajności 2A, 13,8VDC.

Kontroler systemu kontroli dostępu

Do analizy w projekcie przyjeto kontrolery ATS1250. Są to urządzenia kontroli dostępu obsługujące 4 drzwi wspomagające funkcje wyliczone w tabeli Tabela 4-8. Urządzenia są wyposażone w układy sterujące dla urządzeń wykonawczych, odpowiednie zasilanie z podtrzymaniem, zestaw wejść do obsługi standardowych funkcji (monitorowanie drzwi, przycisk wyjścia itp.). Standardowo ATS1250 jest wyposażony w podstawowe rozszerzenie pamięci –

ATS1830 – oraz cztery interfejsy czytników typu Wiegand. Pozwala to realizować wszelkie podstawowe funkcje kontroli dostępu bez dodatkowych rozszerzeń.
MZD kontroli dostępu – ATS1250/60 – posiadają lokalne kopie baz danych użytkowników oraz innych ustawień związanych z kontrolą dostępu. Dlatego reakcja na prezentację karty użytkownika jest natychmiastowa nawet przy dużej liczbie użytkowników.
Podstawowe dane techniczne:
4 przejścia obustronne
4 wejścia bezpośrednie czytników typu Wiegand
16 czytników wyniesionych na magistrali lokalnej
16 linii na płycie MZD
4 wyjścia przekaźnikowe do sterowania zamkami
do 48 wyjść dodatkowych
Zaawansowane funkcje kontroli dostępu
48 makrodefinicji
Pełna kopia lokalna bazy danych użytkowników – praca autonomiczna
Zintegrowany zasilacz impulsowy 3A
Podtrzymanie bateryjne.
Zasilacz modułu będzie wykorzystany do zasilania zamka elektromechanicznego.

Parametr	Wartość
Ilość drzwi	4
Ilość Interfejsów na płycie	4 – czytniki wejściowe drzwi 1 - 4 (lokalnie)
Ilość czytników	16 max.
Magistrala Lokalna	RS485 – jak magistrala systemowa
Zasilacz	4,5A
Baterie	50Ah max.
Wyjścia zamków	Przekaźnik 1A/30V AC
Obudowa	ATS1642 – L
Praca w trybie offline	TAK – pełna funkcjonalność
Linie na płycie	16 (domyślnie przypisane do: 4 czujniki drzwi, 4 przyciski wyjścia, 4 linie DOTL, 4 linie blokowania czytnika)
Pamięć	ATS1830 – zamiennie z IMP ATS1831/32
Serie kart	40
Baza danych	Lokalnie
Antipassback	Lokalnie

Czytnik kart zbliżenowych

Do analizy w projekcie przyjęto czytnik kart zbliżeniowych ATS1190/92.

Podstawowe dane techniczne:

2 diody stanu systemu (programowalne)
Czytnik konfigurowany kartą lub wewnętrznym menu
Sabotaż optyczny oderwania
Możliwość instalacji na zewnątrz
Obudowa wandaloodporna
Interfejs RS485 lub Wiegand wykrywany automatycznie
Wymiary (DxWxG, mm) ATS1190: 36x110x20
Wymiary (DxWxG, mm) ATS1192: 42x150x16
Urządzenie odporne na uszkodzenia mechaniczne i warunki atmosferyczne ze względu wypełnienie obudowy elastycznym wodoodpornym tworzywem. Współpracuje z: Kartami serii ATS147x, programatorem ATS1621. Dodatkowymi akcesoriami Czytnika ATS1190 są wymienne pokrywy obudowy ATS1660 w kolorach białym, czerwonym, szarym, beżowym i czarnym.

Na drzwiach wejściowych do obiektu należy zastosować przycisk czarny. W innych miejscach kolorystykę należy uzgodnić z architektem.

Programator i oprogramowanie

Do analizy w projekcie przyjęto programator ATS1621 lub równoważne i zawiera wszystkie elementy potrzebne do jego użycia:

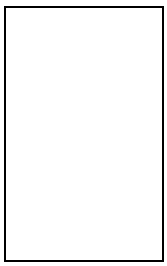
• Programator
• Kable RS232 do podłączenia do komputera
• Zasilacz

Oprogramowanie do obsługi programatora oraz wszelkich aspektów pracy z kartami typu Smart jest integralną częścią programu TITAN. Jest on wyposażony w moduł komunikacji z programatorem zawierającym zabezpieczenia uniemożliwiające nie autoryzowane wykorzystanie sprzętu, narzędzia do programowania kart konfiguracyjnych dla czytników, programowanie kart użytkowników oraz szereg dodatkowych funkcji i narzędzi nie związanych bezpośrednio z kartami smart a służącymi do pracy z kartami w ogóle:

• Moduł Photo ID do zbierania i zachowywania zdjęć użytkowników;

• Możliwość weryfikacji użytkownika – dane z bazy są przywoływane, jeśli użytkownik przechodzi przez drzwi chronione.
• Moduł personalizacji kart z kreatorem szablonów i wsparciem dla drukowania kart wykorzystującym informacje zawarte w bazie danych systemu.
• Aplikacje kredytowe – patrz punkt o niżej – funkcja umożliwiająca użycie czytników poza systemem zabezpieczeń do kontrolowania urządzeń trzecich (dostęp do ksero, kawy, siłowni itd.).
Programator zaprojektowano w pomieszczeniu Dyżurnego Portu 1.60, w pom. operatora SOL 0.14 i na stanowisku wydawania przepustek przy bramie wjazdowej na teren lotniska.

Czujka dualna DD1012AM-D lub równoważne
Czujka dualna 12m,9 kurtyn, PIR+MW, AM,VdS



Zabezpieczenia
Powodami, dla których rozwiązanie systemu kart i czytników programowanych może wydawać się mało bezpieczne są:
• Dostępność sprzętu i oprogramowania do generowania nowych kart – możliwość stworzenia duplikatu karty przez osobę postronną (sabotaż zewnętrzny);
• Możliwość zaprogramowania duplikatu karty przez nieodpowiedzialnego pracownika (sabotaż wewnętrzny);
• Ujawnienie zabezpieczeń w razie utraty karty;
• Ujawnienie zabezpieczeń w razie utraty oprogramowania i/lub sprzętu – programatora.
Zabezpieczenia systemu kart Smart ATS zapewniają wysoki stopień bezpieczeństwa instalacji w której zostały użyte.

Zabezpieczenie sprzętu przed nieautoryzowanym dostępem
Programator łącząc się z komputerem wymaga hasła. Domyślnie hasło jest puste i nie jest sprawdzane, aby ułatwić pracę nowym użytkownikom, kiedy jednak zostanie raz użyte programator zawsze będzie wymagał uwierzytelnienia połączenia hasłem. Hasło połączenia jest

przechowywane tylko w programatorze, co zmniejsza ryzyko ujawnienia hasła połączenia w skutek ataku hakerskiego bądź utraty sprzętu.
Są dwie metody kasowania zawartości pamięci programatora: funkcja programowa oraz użycie karty kasującej programator. O ile funkcja programowa wymaga aby programator był połączony z programem TITAN użycie karty kasującej umożliwia skasowanie pamięci programatora bez użycia komputera. Ze względu na możliwość utraty hasła połączenia (np.: zapominanie, nielojalni pracownicy itp.) zaleca się dołączanie karty kasującej do każdej instalacji zawierającej programator.

Bezpieczeństwo kart

Podstawowym zabezpieczeniem kart i czytników jest 4-ro bajtowy kod zabezpieczający. Jest on programowany na etapie uruchamiania programatora i zapamiętywany w profilu jego ustawień w komputerze oraz w jego pamięci wewnętrznej. Kod zabezpieczenia karty jest zapisywany do każdej programowanej karty użytkownika i karty konfiguracyjnej. Karty konfiguracyjne komunikując się z programowanym czytnikiem oprócz programowanych opcji zapisują w nim również kod zabezpieczający karty. Czytnik ignoruje wszelkie tokeny o innym kodzie zabezpieczającym niż w nim zaprogramowany. Komunikacja czytnik – karta jest dwukierunkowa i szyfrowana. Za każdym razem czytnik odbiera od karty 112 bitów informacji. Każda próba zmiany karty użytkownika już zaprogramowanej wymaga potwierdzenia hasłem. Tylko programowanie kart czystych nie wymaga uwierzytelniania. Dodatkowym zabezpieczeniem jest opcja blokady programowania kodu zabezpieczającego, blokując zmiany tego kodu uniemożliwiamy skasowanie karty. Kod zabezpieczający nie może być odczytany ani z karty ani z czytnika. Można to go odczytać tylko z programatora o ile jest aktywne połączenie z programem TITAN – aktywacja takiego połączenia wymaga autoryzacji.
W profilu programatora definiuje się zakres kodów systemowych kart programowanych dla bieżącego profilu/systemu. W systemie będzie możliwe użycie kart o kodach systemowych z tego zakresu. Jest to dodatkowe zabezpieczenie dla systemów, w których zaprogramowane karty dostarcza instalator.

Unikalność kart.

Dzięki złożeniu kilku parametrów zabezpieczeń wymienionych wyżej:
• Kod zabezpieczający karty posiada 1284 możliwych kombinacji.
• Kody systemowe przyjmują wartości od 0 do 2047
• Numery kart przyjmują wartości od 1 do 65535

Oprogramowanie zarządzające do central ATS Master ATS8300 lub równoważne

Alliance jest korporacyjnym systemem zarządzania bezpieczeństwem w oparciu o urządzenia UTC. Jest to optymalne rozwiązanie dla dużych obiektów. Podstawową rolą, którą pełni aplikacja Alliance jest realizowanie kompleksowego i zintegrowanego stanowiska dozoru, którego zadaniem jest zbieranie i obsługa alarmów i zdarzeń systemowych ze wszystkich urządzeń pracujących na obiekcie.

Podstawowe cechy systemu Alliance:

Aplikacja wielostanowiskowa - maksymalnie 1 serwer + 9 stacji klienckich.

Umożliwia jednoczesną pracę operatorów na wszystkich stanowiskach klienckich.

Obsługa do128 central ATS z wykorzystaniem RS232, PSTN lub IP.

Jednoczesna obsługa do 64 rejestratorów cyfrowych należących do różnych serii produktów (DVMRe, DVSR, SymDec,TVR10,20,40,60,TVN20,TVN60).

Automatyczne wyszukiwanie sekwencji wideo wywołanej alarmem.

Pełna weryfikacja wideo każdego zdarzenia i alarmu.

Wielopoziomowe mapy graficzne do łatwiejszego lokalizowania miejsca alarmów.

Wielostanowiskowość Alliance umożliwia budowanie systemu zarządzania bezpieczeństwem składającego się z kilku niezależnych stanowisk, na których jednocześnie może pracować kilku operatorów.

Operatorzy Ci mogą jednocześnie komunikować się z tymi samymi elementami systemu bez niebezpieczeństwa, że w jakikolwiek sposób wpłyną na pracę innych operatorów. Budowę Alliance oparto o architekturę klient - serwer.

Informacja o produkcie:

Obsługa do 9 klientów

Aplikacja wieloużytkownikowa - równoległa praca kilku operatorów

Monitoring 128 central w oparciu o RS232, PSTN lub IP E

Monitorowanie do 5 systemów sygnalizacji pożaru

Integracja z systemami CCTV po IP

Pełna weryfikacja wideo każdego zdarzenia i alarmu

Możliwość pełnego wczytywania/zapisywania danych

Szerokie spektrum raportów

Zapisywanie zdarzeń w czasie rzeczywistym

Graficzna reprezentacja systemu

Obsługa programatora kart

Moduł PhotoID

Możliwość programowania kart do systemu ATS

Główne cechy aplikacji

Wielostanowiskowość - Alliance umożliwia budowanie systemu zarządzania bezpieczeństwem składającego się z kilku niezależnych stanowisk, na których jednocześnie może pracować kilku operatorów. Operatorzy Ci mogą jednocześnie komunikować się z tymi samymi elementami systemu bez niebezpieczeństwa, że w jakikolwiek sposób wpłyną na pracę innych operatorów.
Budowę Alliance oparto o architekturę klient – serwer. Zakłada ona, że istnieje w systemie jeden dedykowany komputer zwany serwerem, na którym zbierane są wszystkie informacje i dane dotyczące wszelkich zarządzanych urządzeń. Serwer dba o to, aby zapisywać wszelkie komunikaty płynące z urządzeń, znać ich konfiguracje a także dbać o połączenia z nimi.
Komunikacja TCP/IP – cała komunikacja pomiędzy poszczególnymi komponentami systemu jest oparta o sieć TCP/IP. Jest to ewidentne udogodnienie, ponieważ możliwe jest uzyskanie funkcjonalności związanych z integracją central alarmowych z pożarowymi i CCTV bez konieczności stosowania bezpośredniego połączenia przewodowego z wykorzystaniem transmisji szeregowej. Wszystkie informacje i komunikaty przepływające pomiędzy poszczególnymi komponentami systemu są przesyłane siecią komputerową.
Elastyczna baza danych SQL – Alliance służy do zarządzania dużymi systemami posiadającymi wiele modułów rozszerzeń i dodatkowych elementów oraz bardzo dużą liczbę użytkowników. Aby zrealizować zarządzanie taką masą danych projektanci systemu Alliance zdecydowali się wykorzystać relacyjną bazę danych do gromadzenia i zarządzania informacjami o strukturze systemu i jego użytkownikach. W ramach pakietu instalacyjnego operator może wybrać pomiędzy dwoma systemami baz danych MSDE i MS SQL Server w zależności od liczby urządzeń, jakie miałyby być obsługiwane. O ile w przypadku bazy MSDE realnym ograniczeniem jest jej wielkość (około 2GB), o tyle w przypadku wykorzystania bazy danych MS SQL Server nie ma praktycznie żadnych ograniczeń dotyczących pojemności.

Sprzęt komputerowy

Dla zainstalowania aplikacji zarządzającej i obsługi przez operatora zaprojektowano wyposażenie w sprzęt komputerowy: serwer - zlokalizowany w serwerowni SOL oraz stacje robocze zlokalizowane w pomieszczeniu Dyżurnego Portu pom.1.60 (na stanowisku operatora SOL), w pomieszczeniu operatora SOL 0.14, pomieszczaniu SOL 0.83 i dodatkowy dla obsługi bramy wjazdowej od strony wjazdu obsługi. Stanowisko to ma również służyć do obsługi przepustek.

Specyfikacja stacji komputerowych

Wymagania dla serwera:

- wykonanie rack 42'
- Serwer Windows XP,Vista lub Windows 7 (Wersje 32 bitowe), Windows 2008 Server R2 64-bit (Service Pack 1) (tylko na serwer b.danych)
- Intel Pentium IV 3 GHz, min. 3 GB RAM
- 40 GB wolnego miejsca na dysku twardym
- Karta sieciowa 10/100 Mb, napęd CD

Wymagania dla komputera operatora:

- komputer w obudowie monitora jako jednostka zntegrowana
- Klient Windows XP,Vista lub Windows 7 (Wersje 32 bitowe)
- Intel Pentium IV 3 GHz, min. 3 GB RAM

Baza danych:

- Microsoft SQL Server 2008 R2 32-bit Express Edition
- Microsoft SQL Server 2008 R2 32/64-bit

Zamki KD

Do drzwi z kontrolą dostępu zaprojektowane zamki elektromotoryczne rewersyjne (otwarcie w przypadku zaniku napięcia) GEZE IQ LOCK lub równoważne. Są to samoryglujące, wpuszczane zamki paniczne do stosowania w drzwiach na drogach ewakuacyjnych.

Podsawowe dane technchniczne:

- Krzyżowa konstrukcja zapadek i mała odległość pomiędzy zapadkami i ryglem gwarantuje prawidłowe zaryglowanie drzwi przy każdym ich zamknięciu
- Funkcja paniczna gwarantuje, że drzwi zawsze można otworzyć od środka
- Do drzwi profilowych stosowana prostokątna blacha czołowa (szerokość blachy 24mm)
- Do drzwi płaszczowych i drewnianych stosowana zaokrąglona blacha czołowa (szerokość blachy 20mm)
- Rozstaw pomiędzy orzechem a wkładką:
- 92mm do drzwi profilowych
- 72mm do drzwi płaszczowych
- Wysuw rygla w każdym zamku 20mm
- Zabezpieczenie przed wysuwem rygla na otwartych drzwiach

Zaprojektowano zamek IQ typu EL lub równoważne o cechach:

- Trzy tryby pracy:
- Zamknięcie nocne – rygiel wchodzi w ościeżnicę w momencie zamknięcia drzwi
- Tryb dzienny – zapadki „trzymają” drzwi, rygiel jest schowany (naciśnięcie klamki powoduje otwarcie drzwi)
- Otwarcie całkowite – drzwi pozostają niezaryglowane, pchnięcie lub pociągnięcie drzwi powoduje ich otwarcie
- Wszystkie wymagane połączenia do monitorowania stanu drzwi są zintegrowane w zamku EL, dzięki czemu użytkownik zyskuje pełną kontrolę nad położeniem zamka
- Podczas zaniku napięcia rygiel wysuwa się automatycznie, ryglując drzwi
- Podczas zaniku prądu, w sytuacji, gdy drzwi są otwarte, zamek pracuje jak zamek mechaniczny
- Zaryglowanie następuje w mniej niż 1 sekundę
- Zamek posiada styk orzecha, zwarcie styków tego elementu powoduje wywołanie wstępnego alarmu przez system RWS, puszczenie klamki odwołuje alarm
- Obciążalność każdego ze styków w zamku wynosi 0,5A.

Sygnały kontrolno - sterujące zamka:

Numer PIN na kostce	Kolor na kostce przyłączeniowej IQ EM	Kolor na przewodzie przyłączeniowym	Funkcja	Sygnał zwrotny
9	czerwony	czerwony	zasilanie "+24 V DC"	
11	czarny	czarny	zasilanie "- GND"	
12	zielony	zielony	Kontakt klamki NO	Kontakt rozwarty: klamka nie aktywowana (nie jest naciskana)
7	niebieski	niebieski	Kontakt klamki	Kontakt zwarty: klamka aktywowana (została naciśnięta - już przy naciśnięciu 15% pełnego obrotu)
1	zółty	zółty	zasprzęglenie NO	Kontakt rozwarty: zamek zamknięty (klamka niezasprzęglona)
5	pomarańczowy	różowy	zasprzęglenie	Kontakt zwarty: klamka zasprzęglona, drzwi mogą być otwarte za pomocą klamki
10	brązowy	brązowy	Kontakt zapadki pomocniczej NO	Kontakt rozwarty: zapadka nie aktywowana
3	szary	szary	Kontakt zapadki pomocniczej	Kontakt zwarty: zapadka aktywowana

2	biało-brązowy	szaro-różowy	Kontakt wkładki NO / monitoring przewodu zasilającego NC	Kontakt zwarty: wkładka aktywowana / przewód nie uległ uszkodzeniu
4	biało-czarny	czerwono-niebieski	Kontakt wkładki / monitoring przewodu	Kontakt rozwarty: wkładka nieaktywowana / przewód uległ uszkodzeniu
8	biały	biały	Kontakt rygla NO	Kontakt zwarty: rygiel wysunięty
6	fioletowy	fioletowy	Kontakt rygla	Kontakt rozwarty: rygiel nie wys. lub wys. nie całkowicie

Zestawienie materiałów KD i SSW

Można, przy zachowaniu nie gorszych parametrów jakościowych, funkcjonalnych i serwisowych użyć innych niż analizowane elementy. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Lp.	Typ	Opis	Ilość
1	ATS4618E	Centrala alarmowa 16 linii (do 256), 16 obszarów, z dialerem, obudowa z zasilaczem 3A typu L (475 x 460 x 160mm) , z pamięcią 1Mb lub równoważne	2
2	ATS-IP-KIT	Zestaw interfejsów ATS1801 i ATS1809 do komunikacji TCP/IP central ATS Master lub równoważne	2
3	ATS1111	Manipulator LCD 4*16 znaków/16 LED obszarów lub równoważne	2
4	BS129N	Akumulator bezobsługowy 26 Ah, 166x175x125 mm, zaciski śrubowe lub równoważne	2
5	ATS8300	Alliance basic-pakiet z licencją na: 1 serwer (możliwość pracy na serwerze)+1 klient sieciowy PC.Obsługa do 16 rejestratorów CCTV. lub równoważne	1

6	GE-DS-82	Zarządzalny przełącznik Fast Ethernet; desktop/rack, 8 x 10/100MBPS, 2 porty Gigabit TP/SFP lub równoważne	1
7	ATS1251	Moduł kontroli dostępu dla 4 drzwi (do czytników ZAZ,bez wejść Wieganda), obudowa z zasilaczem 12V typu L (ATS1642),8 linii (maks.32) lub równoważne	17
8	ATS1202	Moduł 8 wejść do ekspandera i centrali - PCB lub równoważne	18
9	BS129N	Akumulator bezobsługowy 26 Ah, 166x175x125 mm, zaciski śrubowe lub równoważne	17
10	ATS1192	Czytnik kart zbliżeniowych Hi-tag2 (ZAZ-nie wymaga interfejsu) o podwyższonej wytrzymałości wew/zew, szary z przewodem 2m lub równoważne	97
11		Styk kontrolujący drzwi (konaktron) lub równoważne	64
12	DD1012AM	Czujka dualna 12m,9 kurtyn, PIR+MW, AM lub równoważne	16
13	AS510	Sygnalizator akustyczno - optyczny, zewnętrzny z czerwonym kloszem (możliwość podłączenia akumulatora) lub równoważne	2
14	ATS1475X10	Karty zbliżeniowe Hi-Tag2 (opakowanie 100 sztuk) lub równoważne	200
15	DMN702G	Przycisk wyjścia awaryjnego (typu "Zbij szybkę") zielony konwencjonalny, z zaciskami, podwójny styk, z kluczem testującym, szybką, z puszką lub równoważne	21
16		zamek Geze IQ EL lub równoważne	55
17		serwer zgodnie z opisem	1
18		stacja operatora zgodnie z opisem	4
19	ATS1621	programator kart lub równoważne	3

Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

System zarządzania i monitorowania urządzeń technicznych budynku (BMS)

System sterowania i monitorowania urządzeniami technicznymi budynku. Zadania systemu: Monitorowanie i sterowanie stanami urządzeń technicznych. W systemie zarządzającym - BMS istnieje możliwość ręcznego (za pośrednictwem komputera) sterowania nastawami oraz automatyka - czyli samoczynne zmiany nastaw w zależności od występujących parametrów środowiskowych lub innych urządzeń.

System Zarządzania Bezpieczeństwem

Dla Terminala Portu Lotniczego MAZURY przyjęto do analizy systemu BMS zastosowanie Systemu Zarządzania Budynkiem GEMOS. Można zastosować równoważne rozwiązanie i elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych niz opisane w projekcie oraz spełnienia opisanych w projekcie fnkcji. System BMS zapewnia możliwości centralnego kontrolowania za pomocą komputera lub kilku komputerów wszystkimi komponentami techniki zabezpieczeniowej, przedstawienia meldunków oraz wspomagania realizacji procedur ich obsługi, w wielu przypadkach całkowicie zastępując operatora w wykonywanych czynnościach. Będąc systemem otwartym, pozwoli dostosować się do rozmaitych urządzeń zabezpieczeń, przy czym granice tego dopasowania są bardzo szerokie. Podstawę systemu stanowi komputer, względnie sieć kilku komputerów (do zastosowań wielostanowiskowych). Ponieważ wszystkie nowoczesne centrale sygnalizacyjne wyposażone są w złącze szeregowe, przewidziano podłączenie central do jednego wspólnego systemu informacyjnego zapewniającego prostą obsługę, identyczną dla każdego rodzaju centrali. Połączeń takich dokonano za pomocą interfejsu dopasowującego standard, według którego komunikuje się centrala z otoczeniem, do standardu, w jakim pracuje System GEMOS.

Opis funkcjonalny systemu

System wizualizacji, sterowania i nadzoru, jakim jest system BMS zbiera i analizuje sygnały o stanach takich systemów jak:

- System Sygnalizacji Pożaru (SSP)
- Dźwiękowy System Ostrzegawczy (DSO)
- System Kontroli Dostępu (SKD) i System Sygnalizacji Włamania i Napadu (SSWIN)
- System Nadzoru Wizyjnego (CCTV)
- Wykrywania i Sygnalizacji Pożaru

- Klimatyzacja Obiektu
- Oddymianie grawitacyjne, system zapobiegania zadymieniu na klatkach chodowych
- Sterowanie przewietrzaniem
- Sterowanie oświetleniem

Wszystkie integracje realizowane są na poziomie sprzętowym lub programowym poprzez interfejsy z oprogramowaniem tłumaczącym protokół danego urządzenia lub poprzez bezpośrednie połączenie stykowe.

Na podstawie koncepcji bezpieczeństwa obiektu, przepisów prawnych dotyczących bezpieczeństwa i wymagań klienta ustalana jest lista zdarzeń oraz procedury działań. „Zdarzenia" są to komunikaty przesyłane od zintegrowanych systemów do systemu BMS, którym przypisano różne poziomy ważności w zależności od specyfiki obiektu. Dla usprawnienia pracy operatora systemu rutynowe i statutowe meldunki można zdefiniować w systemie tak, aby były automatycznie opracowywane i protokołowane bez angażowania obsługi. Lista zdarzeń może być w dowolnym momencie dynamicznie modyfikowalna.

Przy opracowywaniu zdarzenia system BMS wspomaga operatora nie tylko szczegółowymi planami sytuacyjnymi z danym alarmującym elementem, ale także wykonuje zdefiniowane procedury automatycznie i prowadzi przez algorytm postępowania dla danej sytuacji. Zadaniem automatycznych procedur działania jest między innymi definiowanie powiązań pomiędzy podsystemami w celu otrzymania kompletnych informacji z alarmowanego miejsca np. w momencie otrzymania alarmu na „monitorze alarmowym" automatycznie prezentowany jest obraz z kamery znajdującej się najbliżej miejsca alarmu czy w momencie alarmu pożarowego system wysyła polecenie sterowania mające na celu ponownego otwarciu drzwi kontroli dostępu.

Procedury postępowania wprowadzane są do systemu jako algorytmy składające się z pojedynczych działań do wykonania, które można łączyć według arytmetyki Boole'owskiej („i" / „lub"). Algorytmy postępowania zawierają nie tylko kolejność i opisy czynności, które należy wykonać, ale także m.in. numery telefonów i dane osób, które należy powiadomić.

Pojedyncze działanie oznacza krok do wykonania np. „wysłanie ochrony do weryfikacji alarmu", „powiadomienie szefa ochrony", „automatyczne otwarcie drzwi". Niejednokrotnie przy opracowywaniu procedur działania często powtarzają się te same czynności, np. „zadzwonić do dyżurnego automatyka (Jan Kowalski tel. 345)". Dla uproszczenia tworzenia procedur działań, takie czynności wprowadzane są tylko raz i mogą one być wielokrotnie wykorzystywane w algorytmach działania. Operator przez plan działania jest informowany, jakie należy podjąć czynności w przypadku określonego zdarzenia. W tym celu pojedyncze czynności planu są jasno i

przejrzyście przedstawiane, oraz muszą być skutecznie wykonane przez operatora, zanim możliwe będzie zdjęcie zdarzenia ze stosów alarmów.

Pojedyncze działania, z którymi zapoznaje się pracownik, mogą być ręczne bądź automatyczne. Działania ręczne mogą zawierać dodatkowy opis tekstowy zawierający szczegółowe informacje dotyczące zadania do wykonania. System, poprzez działania automatyczne, może samodzielnie podjąć zaprojektowane działania. Takim działaniem może być: zaprezentowanie obrazu z kamery, która obejmuje swym zasięgiem miejsce, w którym nastąpiło zdarzenie alarmowe; automatyczne odryglowanie drzwi w systemie kontroli dostępu w reakcji na alarm pożarowy; automatyczne połączenie telefoniczne z centrum kryzysowym; wysłane e-mail lub sms, wydruk planu sytuacyjnego z alarmującym czujnikiem oraz danych o zdarzeniu; uruchomienie i zamkniecie programów zewnętrznych, protokołowanie czy wysłanie dowolnego dopuszczalnego polecenia sterowania do systemu zewnętrznego itd.

Zdarzenia są wprowadzane na tzw. **„stos alarmowy”** według przydzielonego im priorytetu z powiadomieniem akustycznym i wyświetlane na ekranie aż do momentu zakończenia przez obsługę systemu ich opracowywania.

Opracowanie zdarzenia polega na wykonaniu szeregu działań przez użytkownika. Lista tych działań jest wyświetlana na ekranie i zawiera kolejne kroki obsługi meldunku (zdarzenia) zależne od rodzaju zagrożenia. Kroki te to np. „sprawdź miejsce alarmu w celu zweryfikowania alarmu”. Zestaw kroków może być zaprojektowany przez administratora w bardzo rozbudowanej postaci i możliwe są automatyczne współdziałania integrowanych systemów.

Wybierając zdarzenia do opracowania użytkownik widzi plan sytuacyjny tylko z alarmującym czujnikiem, jego opis, czas otrzymania meldunku o alarmie i opisywaną wcześniej procedurę działań, a także wykonane automatyczne działania np. „otwarcie bramy”. Podczas opracowania poszczególnych planów działań operator podaje rezultaty wykonanych działań. Dodatkowo może dodać komentarz. Operator może przerwać opracowywanie zdarzenia i ponownie je wznowić. Wszystkie informacje o zdarzeniu i jego opracowaniu (podjętych działaniach) są protokołowane.

Z poziomu programu można sterować zintegrowanymi systemami. Operator z odpowiednimi uprawnieniami może sam sterować urządzeniami z poziomu programu np. otworzyć lub zablokować drzwi kontroli dostępu czy sterować kamerami. Dzięki zastosowaniu elastycznych możliwości systemu BMS można sposób obsługi i monitorowania zintegrowanych systemów dostosować do poziomu wiedzy i umiejętności osób obsługujących oraz organizacji, co umożliwia nawet nowo przyjętemu pracownikowi na błyskawicznie i bezproblemowe zareagowanie w sytuacji krytycznej.

System BMS może także przechowywane szczegółowe informacje dotyczące elementu wykonawczego czy sprzętu np. informacje dotyczące montażu, protokoły, instrukcje, daty ostatniej konserwacji i termin następnego przeglądu itd.

System BMS automatycznie zapisuje nie tylko dokładne informacje z przychodzących meldunków, wykonane procedury postępowania i komentarze operatora, ale także pozostałe informacje przesyłane od podsystemów czy stacji roboczych. Przechowywane przez system dane historyczne można raportować i analizować wg różnych kryteriów i drukować na formularzach wydruku, które można dowolnie modyfikować.

System posiada wielopoziomowy dostęp do uprawnień połączony z kodami autoryzacyjnymi, co umożliwia różne poziomy ingerencji w system (od pełnej kontroli, poprzez sterowanie urządzeniami, do obsługi zdarzeń), ale także identyfikację osób i rejestrację ich pracy.

Integracja z systemem alarmu włamania i napadu

Sygnały z integrowanego systemu wizualizowane są na planach architektonicznych obiektu oraz na zbiorczych schematach (tablicach synoptycznych). System prezentuje również całą strefę dozorową poprzez jednoczesne informowanie o stanach danej strefy (np. alarm, zazbrojenie/rozbrojenie, zakłócenie). Dzięki temu operator otrzymuje pełniejszą informacje o danej strefie i jej elementach, co pozwala na podjęcie odpowiednich działań zgodnych z procedurą.

Dla każdego elementu systemu zdefiniowane są odpowiednie procedury działania, określany jest plan sytuacyjny oraz **automatyczne sterowania, które sprzęgają działania różnych systemów** np. załączenie obrazu z najbliższej kamery z miejsca, w którym znajduje się alarmujący czujnik. W ramach konfiguracji systemu ochrona może dokonać sterować elementów wykonawczych.

Integracja z systemem kontroli dostępu

W systemie BMS przedstawiane są stany drzwi, a także czujników zamknięcia drzwi, czytników i przycisków w miejscach ich lokalizacji na planach sytuacyjnych (architektonicznych) oraz na schematach zbiorczych. Operator otrzymuje nie tylko informacje o stanie urządzeń systemu kontroli dostępu, ale także informacje o numerze identyfikatora osobistego użytego to odblokowania kontrolowanego przejścia. Z poziomu systemu operator może sterować drzwiami kontroli dostępu np. otworzyć na chwilę, odtworzyć na stałe, zablokować drzwi. Dla każdych drzwi z czytnikami i przyciskami jest zdefiniowana procedura działania, plan sytuacyjny. Sygnały z systemu kontroli dostępu poprzez zdefiniowane automatycznych procedur działania i automatycznych sterowań mogą wywoływać działania innych zintegrowanych systemów. Poziom

integracji zależy od zdefiniowanych potrzeb użytkownika systemu oraz typu wybranego systemu kontroli dostępu.

Integracja z systemem nadzoru wizyjnego

W systemie integrującym wizualizowane są kamery, monitory oraz wyjścia alarmowe w miejscach ich instalacji na planach sytuacyjnych (architektonicznych) oraz na schematach zbiorczych. Specjalny moduł sterowania video pozwala na dowolne przełączanie kamer i monitorów, sterowanie kamerami obrotowymi, zmianę ostrości obrazu i przybliżenia. W systemie definiuje się monitor alarmowy, który jest specjalnie dedykowany do wyświetlania obrazów z kamer, gdy elementy wykonawcze zintegrowanych systemów zgłoszą meldunek (alarm, zakłócenie, uszkodzenie itd.). Operator może również przełączać obrazy z kamer poprzez kliknięcie np. na piktogramy kamer umieszczone na planach sytuacyjnych. Obraz z kamer może być również wkomponowany w układ graficzny aplikacji systemu GEMOS. Z poziomu systemu GEMOS możliwe jest wykonywanie zdjęć obrazów z kamer i gromadzenie ich na serwerze systemowym. Wykonywanie zdjęć możliwe jest w trybie ręcznym (użycie przycisku przez operatora w celu uchwycenia interesującego go zdarzenia obserwowanego przez kamerę), lub w trybie automatycznym realizowanym samoczynnie przez system np. otwarcie drzwi przy użyciu systemu kontroli dostępu będzie wiązało się z wykonaniem i zapisaniem zdjęcia osoby przechodzącej przez przejście.

Integracja z systemem wykrywania i sygnalizacji pożaru

W systemie wizualizacji, sterowania i nadzoru elementy detekcyjne systemu przedstawiane są w miejscach ich rzeczywistego zainstalowania na planach sytuacyjnych oraz na zbiorczych schematach. Dla każdego elementu definiuje się procedury działań, określa szczegółowe plany sytuacyjne. Sygnały przesyłane przez system alarmu pożarowego mogą wywoływać zdefiniowane automatyczne i ręczne procedury działań. Poziom integracji zależy od potrzeb użytkownika i protokołu producenta urządzenia. System może również nadzorować i informować o zadziałaniu elementów automatyki budynkowej uruchamianych przez system alarmu pożarowego.

W przypadku zastosowania interfejsu do centrali Schrack, możliwe będzie wizualizowanie stanu wszystkich czujników, modułów i komponentów wewnętrznych central na wektorowych planach sytuacyjnych, umożliwiających dowolne powiększenie obserwowanego obszaru bez utraty jakości. Możliwe będą także sterowania urządzeniami takie jak blokowanie czujek i stref, testowanie elementów detekcyjnych i wykonawczych oraz potwierdzanie i resetowanie alarmów oraz awarii

Funkcje nadzorujące

1. Stanu akumulatora
2. Stanu zasilania z sieci 230VAC
3. Stanu poziomu dostępu do centrali
4. Stanu wewnętrznego sygnalizatora dźwiękowego
5. Stanu zewnętrznych sygnalizatorów dźwiękowych
6. Stanu drukarek wewnętrznej i zewnętrznej
7. Stanów wejść
8. Stanów wyjść
9. Stanów czujników i ROP-ów
10. Stanu pętli

Funkcje sterujące

1. Wyciszanie wewnętrznego sygnalizatora dźwiękowego
2. Wyłączanie zewnętrznych sygnalizatorów dźwiękowych
3. Kasowanie alarmów
4. Odłączanie pojedynczych czujników lub ROP-ów
5. Ustawianie pojedynczych czujników lub ROP-ów w tryb kontroli
6. Odłączanie grup czujników lub ROP-ów
7. Ustawianie grup czujników lub ROP-ów tryb w kontroli
8. Odłączanie pętli
9. Odłączanie wyjścia
10. Odłączanie wejścia
11. Ustawianie wejścia w tryb kontroli

Integracja z dźwiękowym systemem ostrzegawczym

System BMS umożliwi wizualizację wszystkich elementów systemu DSO wraz z ich lokalizacją na planach sytuacyjnych i technicznych. Odwzorowanie stanów kontrolerów, wzmacniaczy, zasilania sieciowego i awaryjnego, użycie i stan pulpitu mikrofonowego.

System integrujący zapewni także nadawanie komunikatów alarmowych i komercyjnych, regulację głośności i przyłączanie źródeł dźwięku do dowolnych stref nagłośnieniowych.

Integracja z systemem klimatyzacji

Do systemu integrującego zbierane będą informacje o bieżącej temperaturze w pomieszczeniach wyposażonych w klimakonwektory.. W zależności od wartości zmierzonych operator zostanie

poinformowany o zdarzeniu i zostaną podane odpowiednie procedury działania (algorytmy postępowania). Za pośrednictwem interfejsu komunikacyjnego pomiędzy systemem GEMOS a sterownikami klimakonwektorów możliwe będzie dokonanie korekty nastaw, włączeni lub wyłączenie urządzeń. Sterowniki klimakonwektorów umożliwiają wymianę informacji wykorzystując protokół modus. Sterowniki należy połączyć ze switchem systemowych BMS zrównoleglоną magistralą RS-485 wykonaną za pomocą kabla typu FTP kat 5.

Integracja z systemem oddymiania grawitacyjnego

W celu umożliwienia sterowania funkcją przewietrzania oraz pełnego monitoringu centralek okien oddymiających projektuje się interfejs do centralek oddymiających. Interfejs jest przeznaczony do integracji centrali oddymiania oddymiających z systemem BMS. Interfejs ma postać karty (sterownik Master) z odpowiednim oprogramowaniem (firmware). Umożliwia on monitorowanie stanu centrali oddymiającej oraz sterowanie klapami/siłownikami do niej podłączonymi. Interfejs nie posiada dodatkowego oprogramowania służącego do jego konfiguracji. Wszystkie czynności konfiguracyjne są przeprowadzanie z poziomu systemu BMS. Centralki oddymiające należy połączyć ze sterownikiem MASTER zrównoleglоną magistralą RS-485 wykonaną za pomocą kabla typu FTP kat 5. Sterownik MASTER został zlokalizowany w szafie serwerowej w serwerowni SOL. Sterownik MASTER zasilany napięciem 12V z dedykowanego zasilacza buforowanego.

Integracja z systemem oświetlenia

W pomieszczeniu 1.63 należy zainstalować szafkę teletechniczną wiszącą dwusekcyjną, w której zamontowane zostaną karty wejść BMS (7 sztuk). Kart zostaną połączone za pomocą kabli teletechnicznych typu YTKSY 5x2x0,8 z modułami wejściowymi DALI lub równoważnym w rozdzielnicach RO2, RA8 i A01. Karty wejść BMS powinny zostać połączone do modułu IP Gateway umieszczonego w szafie serwerowej BMS za pomocą kabla magistralnego typu YTKSY 1x2x0,8 ekw. Z poziomu stacji roboczej BMS możliwe będzie sterowanie obwodami oświetleniowymi (włącz/wyłącz) w sposób ręczny lub automatyczny (np. o określonej godzinie, na skutek konkretnych zdarzeń pochodzących ze zintegrowanych systemów).

Zaprojektowane rozwiązanie

Celem instalacji Systemu zarządzania bezpieczeństwem BMS, jest zwiększenie bezpieczeństwa Terminala, poprzez zintegrowanie wszystkich instalacji bezpieczeństwa w jednym wspólnym systemie informacyjnym.

Z uwagi na ilość zaprojektowanych interfejsów, dla obiektu przewidziano system BMS w wersji STANDARD, która charakteryzuje się:

- 2000 punktów na integrowane systemy.

  Oznacza to, iż licencja bazowa, ogranicza do 2 000 elementy liniowe, wszystkich integrowanych systemów, SSP ,KD , SSWIN , CCTV itp., które mogą być zdefiniowane w systemie.

Istnieje możliwość rozszerzania licencji kolejnymi pakietami po 500 lub 1 000 elementów.

- 2 stanowiska robocze.

  Oznacza to, iż system może być obsługiwany jednocześnie na dwóch stanowiskach roboczych.

  Istnieje możliwość rozszerzania licencji o kolejne stanowiska robocze.

- 100 procedur.

  Oznacza to, iż możliwe jest wprowadzenie do systemu 100 procedur działań na wypadek zdarzenia, czyli czynności działania.

  Istnieje możliwość rozszerzania licencji pakietem po 100 kolejnych procedur.

- 100 akcji

  Oznacza, to iż w systemie możliwe jest wprowadzenie akcji, które są podłączone pod zdefiniowane procedury, inaczej kroki, jakie należy wykonać na wypadek zdarzenia.

  Istnieje możliwość rozszerzania licencji pakietem po 100 kolejnych akcji.

- 100 czujników strefowych.

  Oznacza to, iż możliwe jest w systemie zdefiniowanie wirtualnych czujników stref, pod które podpina się czujniki rzeczywiste. Funkcjonalność umożliwia śledzenie stanu zbiorczego wszystkich czujników.

- 100 planów sytuacyjnych.

  Oznacza to, iż możliwe jest zdefiniowanie w systemie podkładów budynków, na które nanoszone są czujniki. Każda warstwa z czujnikami stanowi osobny plan sytuacyjny

  Istnieje możliwość rozszerzania licencji pakietem po 100 kolejnych planów.

- 1 magistrala systemowa BUS

  Oznacza to, iż możliwe podłączenie do systemu jednego modułu komunikacyjnego ETHERNET GATEWAY obsługującego do 127 kart wejść i wyjść przeciwpożarowych łącznie.

  Istnieje możliwość rozszerzania licencji o możliwość obsługi dodatkowych magistral.

Dla Terminala Portu Lotniczego MAZURY przewiduje się zaprojektowanie jednej stacji roboczej systemu BMS – stacja główna zarządzająca całym obiektem mieszcząca się na stanowisku

operatora SOL w pomieszczeniu 1.60 (Pomieszczenie Nadzoru) z możliwością dołączenia kolejnej, dodatkowej stacji rezerwowej mogącej również pełnić funkcję stacji serwisowej dla pracowników serwisu systemu. Niezależnie udostępniona będzie również możliwość połączenia się zdalnego za pośrednictwem sieci WWW. Wszystkie stacje robocze pełnić będą funkcję klienta serwera na którym zostanie zainstalowany główna aplikacja.

Stacja robocza, pracująca w trybie on-line 24h/dobę wyposażona zostanie w dwa monitory LCD o przekątnej ekranu minimum 22" i rozdzielczość 1920x1800 pikseli. Rozwiązanie takie pozwoli na optymalną wizualizację i zapewni wymagany komfort obsługi systemu.
Taki układ zapewnia przejrzyste nawigowanie po mapach wektorowych całego obiektu, bez konieczności stosowania „wycinków" terenu, co jest spotykanym rozwiązaniem w przypadku grafik bitmapowych (rastrowych). Do stanowiska SOL powinny być przekazywane wszystkie informacje z systemów bezpieczeństwa obiektu

Komputer - serwer systemu zarządzania bezpieczeństwem będzie połączony za pomocą interfejsów wykorzystujących technologię TCP/IP z interfejsami integrowanych systemów, także ze sterownikiem MASTER służącym do integracji z centralkami oddymiającymi. Do drukowania nadchodzących zdarzeń zainstalowana zostanie drukarka, jednocześnie wszystkie zdarzenia będą protokołowane na twardych dyskach serwera. Zarówno stacje robocze jak i serwer systemu zasilane powinny być ze źródła napięcia gwarantowanego. Serwer zostanie umieszczony w szafie serwerowej 19"42U w pomieszczeniu 1.50 (Serwerownia SOL).

Zarówno serwer system, stacja robocza jak i wszystkie interfejsy zostaną podłączone do wspólnej wydzielonej sieci teleinformatycznej. Sieć teleinformatyczna jest przedmiotem odrębnego opracowania.

Minimalne parametry serwera i stacji roboczej:
Stacja robocza
Processor : 3rd Gen Intel Core i3-3220 Processor (Dual Core, 3.30GHz, 3MB, w/ HD2500 Graphics)
E-Star : No ESTAR Settings Ship Accessory : Polish Docs with European Power Cord
Dysk DVD z zasobami : OptiPlex 9010 diagnostyka i sterowniki
Ship Mod : OptiPlex Intel Core i3 Label
Memory : 4GB (1X4GB) 1600 MHz DDR3 Non-ECC

Hard Drive : 250GB 3.5inch Serial ATA III (7.200 Rpm) Hard Drive
Optical Drive : 16XDVD+/-RW Drive
Optical software not required - OS software sufficient
Cable and bracket : for primary hard drive 3.5inch
Cable and bracket : for no additional hard drive
Karta graficzna : 1GB AMD Radeon HD 7470 (pełna wysokość, 1DP i 1DVI-I)
Adapter : Display Port to DVI (1920x1200) Adapter for Dell Systems
Speakers : Internal Dell Business Audio Speaker
Mice : Dell Laser Scroll USB (6 Buttons) Silver and Black Mouse
Keyboard : US/European (QWERTY) Dell KB212-B QuietKey USB Keyboard Black
Operating System : kompatybilny z systemem BMS (64Bit) Polish
MS Media : Resource DVD
Brak oprogramowania biurowego
No Out-of-Band Systems Management,
Operating System Recovery Dell Backup and Recovery Manager for SO
Additional Software : 7
24" LED monitor VGA,DVI-D (1920x1080) Black

Serwer
Procesor Intel Xeon E5-2650 2,00GHz, 20MB pamięci podręcznej, 8,0GT/s QPI, Turbo, 8 rdzeni, 95W
Obudowa z maks. 8 dyskami twardymi 3,5 cala i 4 dyskami PCIe SSD, konfigurac do szafy serwerowej
1333MHz moduły RDIMM
8GB pamięci RDIMM, 1333 MHz, niskie napięcie, dwa banki, x4
Intel Xeon E5-2650 2,00GHz, 20MB pamięci podręcznej, 8,0GT/s QPI, Turbo, 8 rdzeni, 95W
VFlash, 8GB karta SD do rozwiązania iDRAC Enterprise
300GB SAS 6GB/s 15 000obr./min 3,5-calowy dysk twardy Hot Plug
Konfiguracja bezdyskowa przy użyciu półprzewodnikowych dysków PCIe Express Flash
PERC H710 kontroler adaptera RAID, 512MB nieulotnej pamięci podręcznej
WEWNĘTRZNY DVD+/-RW, SATA
Europejski 220V zapasowy przewód zasilający
Podwójny nadmiarowy wymieniany bez wyłączania systemu zasilacz (1+1), 1100W
Kabel do kontrolera PERC serwera T620 do 2,5-calowej obudowy

USB mysz optyczna

Keyboard : US/Euro (QWERTY)

Szyny wsuwane ReadyRails do szafy serwerowej z wysięgnikiem do mocowan kabli do konfiguracji szafy

iDRAC7 Enterprise

Aktywny kontroler zasilania ustawienie BIOS

No Media Required

Sysyem Operacyjny Servera kompatybilny z BMS

Zestawienie materiałów

Dla Terminala Portu Lotniczego MAZURY przyjęto do analizy systemu BMS zastosowanie Systemu Zarządzania Budynkiem GEMOS. Można zastosować równoważne rozwiązanie i elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych niz opisane w projekcie oraz spełnienia opisanych w projekcie fnkcji. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Zestawienie licencji

Lp	Typ	Ilość	Opis
1	LIC-ES-GMS_STA	1	SYSTEM ZARZĄDZANIA BUDYNKIEM GEMOS-Standard lub równoważne
2	LIC-ES-GMS_D_1	1	INTERFEJS STANDARDOWY-(SSP) lub równoważne
3	LIC-ES-GMS_D_2	1	INTERFEJS NIESTANDARDOWY (DSO) lub równoważne
4	LIC-ES-GMS_D_2	1	INTERFEJS NIESTANDARDOWY-(CCTV) lub równoważne
5	LIC-ES-GMS_D_1	1	INTERFEJS STANDARDOWY (SKD) lub równoważne
6	LIC-ES-GMS_D_1	1	INTERFEJS STANDARDOWY (SWIN) lub równoważne
7	LIC-ES-GMS_D_2	1	INTERFEJS NIESTANDARDOWY (MODBUS – KLIMAKONWEKTORY) lub równoważne
1	LIC-ES-GMS_D_1	1	INTERFEJS STANDARDOWY (ODDYMIANIE) lub równoważne
8	LIC-ES-GSWG4	3	ROZSZERZENIE LICENCJI DANYCH BAZOWYCH o 1000 czujn. lub równoważne

Zestawienie urządzeń

Dla Terminala Portu Lotniczego MAZURY przyjęto do analizy systemu BMS zastosowanie Systemu Zarządzania Budynkiem GEMOS. Można zastosować równoważne rozwiązanie i elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych niz opisane w projekcie oraz spełnienia opisanych w projekcie fnkcji. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Lp	Typ	Ilość	Opis
1	serwer	1	SERWER BMS zgodnie z opisem
2	stacja robocza	2	Stacja Robocza dwumonitorowa zgodnie z opisem
3	drukarka	1	DRUKARKA igłowa o szerokości wydruku 80 kolumn w trybie normalnym i rozdzielczości 240x216 dpi
4	przełącznik	1	zarzadzalny rzełącznik, 24 Port GE, 2 GE/SFP
5	K19	1	KASETA 19" Z WYPOSAŻENIEM DO KART BMS lub równoważne
6	ST-M	1	STEROWNIK MASTER z PORTEM ETHERNET
7	Z12/10	1	ZASILACZ BUFOROWY 230V/12V 10A
8	AKU	1	AKUMULATOR 12V/28Ah

Można zastosować równoważne elementy innych producentów pod warunkiem zapewnienia nie gorszych parametrów technicznych i jakościowych niż przyjęte w projekcie. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

System transportu bagażu (BHS)

Projektowane systemy zapewniają w części odlotowej i przylotowej:

- transport bagaży rejestrowych i nadwymiarowych wraz z odczytem informacji o bagażach oraz ich śledzeniem;
- kontrolę bezpieczeństwa bagaży rejestrowanych i nadwymiarowych;
- kontrolę celną bagaży rejestrowanych;
- kontrolę radiometryczną bagaży rejestrowanych i nadwymiarowych;
- kontrolę bezpieczeństwa bagaży podręcznych i pasażerów wraz z możliwością wykrywania płynnych materiałów wybuchowych (LEDS);
- kontrolę radiometryczną bagaży podręcznych i pasażerów;
- kontrolę bezpieczeństwa personelu.

Zaprojektowany system transportu bagażu rejestrowanego przewiduje 4 stanowiska odprawy z czego jedno stanowisko jest podwójne: obsługuje również bagaż ponadwymiarowy. przewidziano rezerwę miejsca na dwa stanowiska odpraw i system transportu bagażu jest tak zaprojektowany, aby nie wymagał znaczących przeróbek przy rozbudowie.

Obliczenia długości taśmociągów i czasu reakcji obsługi:

2 poziom kontroli długość taśmociągów 8,5 m- 17s; - prędkość 0.5 m/s

3 poziom kontroli długość taśmociągów 6,25m - 17s - prędk. 0,37m/s.

Szczegółowe dane systemy BHS znajdą się w projekcie wykonawczym.

Systemy bezpieczeństwa bagażu i pasażerów

Wielopoziomowy system bezpieczeństwa kontroli bagażu rejestrowanego.

Wielostopniowym system oparty jest na dwuwidokowym urządzeniu RTG o minimalnych wymiarach tunelu szer.1000mm wys. 800mm Obrazy w urządzenia wysyłane są na kolejne poziomy do podjęcia decyzji przez operatora.

Poziom I – co najmniej dwuwidokowe urządzenie RTG

Poziom II (bezpieczeństwa) - stacje analiz z funkcją TIP (min. 2 szt.) obrazy z urządzenia Poziom I, wysyłane są na pierwszą „wolną” stację operatorską,

Poziom III (bezpieczeństwa) - stacja analiz z funkcją TIP (min. 1szt)

Poziom IV (bezpieczeństwa) - stacja ponownej kontroli (min 1 szt.) wyposażona w czytnik kodów kreskowych. Za pomocą czytnika kodów, po zeskanowaniu nalepki na bagażu zostaje wywołany

obraz z urządzenia RTG poziomu I. (Aby zapewnić pełna funkcjonalnośc systemu) przed urządzeniem Poziomu I konieczny jest zamontowanie skanera 360 stopni
Poziom II (kontrola celna) - stacja analiz (min. 1szt)
Poziom IV (kontrola) - stacja ponownej kontroli (min 1 szt.) wyposażona w czytnik kodów kreskowych.
System wyposażony w stacjonarny monitor promieniowania gamma i neutronowego.

System kontroli bagażu ponadwymiarowego

Oparty jest o urządzenie dwuwidokowe urządzenie RTG o minimalnych wymiarach tunelu szer. 1000mm, wys. 1000mm. Urządzenie w razie awarii urządzenia poziomu I jest również backupem systemu kontroli bagażu rejestrowanego. Układ taśmociągów BHS pozwala na zmianę kierunku trasy bagażu.
System wyposażony w stacjonarny monitor promieniowania gamma i neutronowego.

Punkt kontroli bagażu podręcznego, pasażerów i przejścia służbowe

Przejście dla pasażerów:

zaprojektowano dwa przejścia i rezerwę miejsca na jedno dodatkowe przejście. Wejście do strefy kontroli wyposażone w stacjonarny monitor promieniowania gamma i neutronowego. Każde przejście dla pasażów wyposażone w dwuwidokowe urządzenie rentgenowskie (o minimalnych wymiarach tunelu ser. 600mm, wys. 400mm) z możliwościa kontorli płynów (LEDS) (min. standard II, typ C) oraz bramowy wykrywacz metali WTMD (min. Standard II). Dodatkowo urządzenie do kontorli płynów LEDS (min. Standard II typ B, min. Standard II typ A) płynów wspólne dla wszystkich przejść przy stanowisku SOL. Zamawiający dopuszcza zastosowanie dwóch oddzielnych urządzeń do kontorli płynów LEDS (min. Standard II typ B, min. Standard II typ A).

Przejście dla pasażerów VIP:

zaprojektowano przejścia dla pasażerów VIP i załogi pokładowej. Wejście do strefy kontroli wyposażone w stacjonarny monitor promieniowania gamma i neutronowego. Przejście wyposażone w dwuwidokowe urządzenie rentgenowskie (o minimalnych wymiarach tunelu ser. 600mm, wys. 400mm) z możliwościa kontroli płynów (LEDS) (min. standard II, typ C) oraz bramowy wykrywacz metali WTMD (min. Standard II).

Przejście służbowe:

zaprojektowano przejście służbowe dla personelu obsługi lotniska.

wyposażone w dwuwidokowe urządzenie rentgenowskie (o minimalnych wymiarach tunelu ser. 600mm, wys. 400mm) z możliwościa kontroli płynów (LEDS) (min. standard II, typ C) oraz bramowy wykrywacz metali WTMD (min. Standard II).

Przyloty kontrola celna

Oparta jest o jednowidokowe urządzenie RTG o minimalnych wymiarach tunelu szer. 1000 mm, wys. 100100mm, zintegrowane z systemem BHS.

Przyloty kontrola radiometryczna

Stacjonarne monitory promieniowania - tzw. bramki radiometryczne projektowane są w miejscach związanych z potrzebą precyzyjnej kontroli osób, bagażu lub towarów przemieszczających się przez strefę kontroli, na obecność materiałów radioaktywnych i jądrowych.
System składa się z jednej lub dwóch kolumn pomiarowych realizujących funkcję detekcji i wstępnej obróbki sygnałów, panelu operatorskiego z ekranem dotykowym i drukarką oraz oprogramowania komputerowego do zdalnego zarządzania system stacjonarnych monitorów promieniowania.
Interaktywny panel operatorski komunikuje się z kolumnami pomiarowymi, przetwarza otrzymane sygnały i realizuje zaimplementowane algorytmy funkcjonalne i decyzyjne. Panel operatorski komunikuje się dwukierunkowo: zdalnie kontroluje kolumnę pomiarową oraz pozwala na zdalną zmianę parametrów. Umożliwia wizualizację, generowanie i wydruk raportów automatycznie lub na żądanie.
Zdalny system zarządzania zainstalowany na dedykowanym serwerze wraz aplikacjami klienckimi zainstalowanymi na komputerach osobistych jest przeznaczony do kontroli obiektów poruszających się w wyznaczonych strefach oraz do kontroli pracy urządzeń. Nadzorem objęte są wszystkie stacjonarne monitory promieniowania połączone w jednej sieci ethernetowej.

Przy wjeździe wózków z bagażem rejestrowym zaprojektowano stacjonarny monitor promieniowania gamma i neutronowego. W przypadku wykrycia substancji zastrzeżonej urządzenie identyfikuje wózek, a identyfikację bagażu trzeba przeprowadzić ręcznie.
Przy wejściach dla pasażerów do strefy Schengen i non Schengen zaprojektowano stacjonarne monitory promieniowania gamma i neutronowego.

Integracja

Wszystkie urządzenia RTG mają być połączone w system pozwalający na między innymi powadzenie statystyk dotyczące kontroli bezpieczeństwa, zarządzanie funkcją TIP, dodawanie i

usuwanie loginów operatorów. Jeśli jest to wymagane przez producenta należy dostarczyć serwer, który zapewni taką funkcjonalność.
Bramowe wykrywacze metali WTMD muszą być połączone w system pozwalający na prowadzenie statystyk.

Szczegółowy opis systemu BHS i systemów bezpieczeństwa

Założenia sytemu

Przedmiotem niniejszego postępowania jest zaprojektowanie, dostawa, montaż, uruchomienie i przeprowadzenie niezbędnych uruchomień, testów, szkoleń, opracowanie dokumentacji powykonawczej, dostawa niezbędnych części zamiennych oraz udzielenie gwarancji jakości na wielopoziomowy system kontroli i transportu bagażu rejestrowanego, bagażu podręcznego oraz pasażerów i personelu. Oferowany system transportu bagaży powinien być w pełni zintegrowany z systemem kontroli bezpieczeństwa bagażu rejestrowanego oraz systemem kontroli radiometrycznej. Do obowiązków Wykonawca należy przeprowadzenie pełnej integracji systemu transportu z urządzeniami rentgenowskimi i urządzeniami kontroli radiometrycznej. Wykonawca zobowiązany jest również dokonać wszelkich niezbędnych uzgodnień z Zamawiającym, w tym w szczególności służbami lotniskowymi (SOL, Straż Graniczna, Służba Celna) w odniesieniu do funkcjonalności oferowanego systemu. System będzie instalowany w nowo powstałym Terminalu Pasażerskim Portu Lotniczego Mazury Zamawiający udostępni projekty powykonawcze budowlane, w tym m.in. projekty instalacyjne i architektury).
Oferowane systemy powinny zapewnić w części odlotowej:

- transport bagaży rejestrowanych i rejestrowanych nadwymiarowych wraz z odczytem informacji o bagażach rejestrowanych na odlotach
- kontrolę bezpieczeństwa bagaży rejestrowanych i nadwymiarowych;
- kontrolę celną bagaży rejestrowanych;
- kontrolę radiometryczną bagaży rejestrowanych i nadwymiarowych;
- kontrolę bezpieczeństwa bagaży podręcznych i pasażerów wraz z możliwością wykrywania płynnych materiałów wybuchowych (LEDS);
- kontrolę radiometryczną bagaży podręcznych i pasażerów;
- kontrolę bezpieczeństwa personelu.

Rolety listwowe oddzielające strefy: publiczną od zastrzeżonej wchodzą również w zakres dostawy BHS.

Opis funkcjonalny systemu transportu i kontroli bagaży rejestrowanych i nadwymiarowych, podręcznych oraz pasażerów i personelu

Wielopoziomowy system transportu i kontroli bagaży rejestrowanych na kierunku odloty

Bagaże rejestrowane będą odprawiane na 4 stanowiskach odpraw biletowo- bagażowych. Wszystkie stanowiska odpraw biletowo- bagażowych wyposażone będą w dwuczęściowe taśmociągi: wagowy i odsyłający. Pasażer umieszcza swój bagaż na taśmociągu wagowym, a waga bagażu jest prezentowana na dwóch wyświetlaczach (jeden dla pasażera, drugi dla operatora) ze wskazaniami z zakresu 0-150kg i dokładnością 100g. Operator drukuje etykietę bagażu z kodem paskowym zgodnym ze standardem IATA (drukarka kodów paskowych jest składową stacji operatorskiej firm handlingowych, poza zakresem Wykonawcy systemu transportu i kontroli bagażu). Etykieta jest ręcznie nakładana na bagaż przez operatora. Następnie, operator, wybierając przycisk z panelu operatorskiego, przesyła odprawiony bagaż na taśmociąg odsyłający. Tutaj bagaż czeka na wolne okno na taśmociągu zbiorczym. System śledzący z dedykowanymi oknami zapewnia równomierne przekazywanie bagaży ze wszystkich stanowisk odpraw biletowo-bagażowych do systemu transportu i kontroli.

Za taśmociągami zbiorczymi zamontowany jest skaner 360 stopni, który sczytuje kody kreskowe bagaży, co zapewnia ich pełne śledzenie i monitorowanie w systemie.

Każdy bagaż wprowadzony do systemu jest uznawany za ‘niebezpieczny’ i poddany kontroli bezpieczeństwa, realizowanej przy pomocy co najmniej dwuwidowkowego urządzenia rentgenowskiego (min. wymiary tunelu szer. 1000mm wys. 800mm). Przed urządzeniem rentgenowskim zainstalowana jest bramka kontroli wysokości, weryfikująca wysokość bagaży. W przypadku gdy bagaże przekraczają zadane limity pod względem wysokości (przekraczają wymiary tunelu urządzenia rentgenowskiego), transporter na którym się znajdują zostaje zatrzymany, a operator ręcznie usuwa bagaż z systemu. Obrazy bagaży prześwietlnonych na urządzeniu RTG Poziom I są wyświetlane na stacjach operatorskich Poziomu II. Obrazy bagaży uznanych za niebezpieczne są wyświetlane na stacjach operatorskich poziomu II. Operator dysponuje zadanym czasem minimum 17 sekund na podjęcie decyzji co do statusu kontrolowanego bagażu. Bagaże uznane za bezpieczne kierowane są taśmociągami do sortowni docelowo na transporter rolkowy znajdujący się na końcu linii. Bagaże uznane za niebezpieczne i te, co do których operator nie podjął decyzji, kierowane są dwukierunkowym transporterem na III poziom kontroli bezpieczeństwa. Na III poziomie kontroli, operatorzy mają możliwość ponownej analizy obrazów, wygenerowanych przez urządzenie rentgenowskie I poziomu. Bagaże uznane za

bezpieczne są ponownie wprowadzane do systemu dwukierunkowym transporterem i kolejno transportowane do sortowni na transporter rolkowy. Bagaże uznane za niebezpieczne są kierowane na IV poziom kontroli- kontrola manualna w obecności pasażera. Na IV poziomie kontroli, operator ma do dyspozycji widok bagażu z urządzenia Poziomu I. Obraz wywoływany jest na stację ponownej kontroli za pomocą czytnika kodów IATA. Bagaże uznane za bezpieczne po kontroli manualnej są z powrotem wprowadzane do systemu transporterem dwukierunowym i do sortowni na transporter rolkowy. Bagaże uznane za stwarzające zagrożenie bombowe są kierowane, za pośrednictwem dwukierunkowych transporterów, na stanowisko pirotechnika, celem neutralizacji (pojemnik pirotechniczny poza dostawą Wykonawcy systemu transportu i kontroli). Bagaże, które trafiły do sortowni są manualnie sortowane i ładowane na wózki bagażowe przez pracowników handlingowych i kolejno wywożone z sortowni do załadunku do samolotu. Przy wyjeździe z sortowni zainstalowana jest waga najazdowa do ważenia wyjeżdżających, załadowanych wózków bagażowych. W ramach zamówienia należy zaprojektować i zamontować wagę wbudowaną w warstwy posadzkowe zlokalizowaną przy wyjeździe z sortowni. Parametry wagi: Waga najazdowa zagłębiona w warstwach posadzkowych o wymiarach min 2 x 3 m i udźwigu min. 4000 kg.

Każdy bagaż wprowadzony do systemu transportu będzie poddany kontroli radiometrycznej, celem wykrycia ewentualnych materiałów radioaktywnych.

Bagaże o statusie bezpiecznym będą mogły być poddawane kontroli celnej na podstawie obrazów wygenerowanych przez urządzenie rentgenowskie I poziomu kontroli. System powinien zakładać przesyłanie 100% obrazów bagaży na stacje operatorskie kontroli celnej.

Kontrola celna odbywa się również za pośrednictwem urządzenia poziomu I. Przewidziana jest minimum jedna stacja operatorska na poziomie II (dla kontorli celnej),. Bagaże co do których nie została podjęta decyzja negatywna są kierowane do samolotu. Bagaże, które zostały zakwestionowane przez operatora służby celnej są kierowane do ponownej kontroli (pomieszczenie kontroli manualnej na IV poziomie). Ponowna kontrola odbywa się w obecności pasażera. Operator ma do dyspozycji obraz bagażu, wygenerowany przez urządzenie I poziomu na dedykowanej stacji ponownej kontroli celnej. Obraz wywoływany jest za pomocą czytnika kodów IATA.

Redundancja wielopoziomowego systemu kontroli i transportu bagaży rejestrowanych na kierunku odloty

Wielopoziomowy system kontroli i transportu bagaży rejestrowanych zapewnia pełną redundancję. W przypadku awarii urządzenia rentgenowskiego poziomu I, bagaże rejestrowane odprawione na

stanowiskach odpraw biletowo- bagażowych są kierowane taśmociągami zbiorczymi na linię dedykowaną bagażom nadwymiarowym. Bagaże są kontrolowane pod kątem bezpieczeństwa przez urządzenie rentgenowskie w linii bagaży nadwymiarowych. Bagaże uznane za bezpieczne transportowane są sorterem poziomym i taśmociągiem łączącym do linii głównej transportu i kontroli bagaży rejestrowanych, skąd kierowane są do sortowni. Bagaże uznane za niebezpieczne są kierowane do kontroli manualnej na IV poziom kontroli, za pośrednictwem sortera poziomego i taśmociągu łączącego się z linią główną. Operator analizuje obrazy bagaży wyświetlane na konsoli operatorskiej i podejmuje decyzję co do statusu każdego bagażu, kierując go odpowiednio do kontroli manualnej lub sortowni (wybierając stosowny przycisk z konsoli operatorskiej).
Bagaże nadwymiarowe mogą być odprawiane wyłącznie w trybie ‘zwykłym’.

System transportu i kontroli bagaży nadwymiarowego na kierunku odloty

Bagaż nadwymiarowy jest przyjmowany na oddzielnym stanowisku odpraw biletowo-bagażowych. Stanowisko odpraw wyposażone jest w dwuczęściowe taśmociągi, pierwszy z wbudowaną wagą. Po odprawie, bagaż nadwymiarowy jest kierowany do kontroli bezpieczeństwa przeprowadzanej przy pomocy dwuwidokowego urządzenia rentgenowskiego o min wymiarach tunelu szer. 1000mm wys. 1000 mm. Bagaże nadwymiarowe zawsze są odprawiane w trybie ‘zwykłym’ systemu. Obrazy bagaży są wyświetlane na konsoli operatorskiej. Operator podejmuje decyzję co do statusu każdego bagażu. Bagaże uznane za bezpieczne są kierowane na wprost do załadunku na wózki bagażowe. Bagaże niebezpieczne są wycofywane z powrotem na początek linii do kontroli manualnej w obecności pasażera. Odprawa bagaży nadwymiarowych odbywa się zawsze przy asyście uprawnionego operatora. Bagaże nadwymiarowe muszą być odprawiane sukcesywnie, aby zapewnić ewentualny powrót bagażu niebezpiecznego na początek linii, unikając blokowania się bagaży.
Każdy bagaż wprowadzony do systemu transportu będzie poddany kontroli radiometrycznej, celem wykrycia ewentualnych materiałów radioaktywnych.

Wymogi dla urządzeń do kontroli bagażu rejestrowanego POZIOM I

- Wymiary tunelu min. 1000mm x 800mm
- Dwa widoki (dwa generatory) pod różnymi kątami (widok z dołu i boku urządzenia)
- Prędkość taśmociągu: minimum 0,2m/s
- Wysokość taśmociągu dostosowana do wysokości urządzenia
- Penetracja stali: min 35 mm
- Rozdzielczość: min 39 AWG

- UPS umożliwiający zamkniecie komputera na wypadek awarii zasilania
- Funkcja TIP (1000 obrazów)
- Zasilanie 230 Vac/50/60Hz
- Zakres temperatury pracy 5-40°C
- Walizka testowa
- Komunikaty urządzenia w języku polskim
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Interfejs pozwalający na integracje z systemem transportu bagażu
- Interfejs pozwalający na pracę urządzenia w systemie zarządzania urządzeniami RTG
- Znak CE

Stacje operatorskie POZIOM II (bezpieczeństwo)

Wymagane są minimum 2 stacje.

Obraz będzie wyświetlany na pierwszej wolnej stacji operatorskiej

Stacja powinna być wyposażona:

- Klawiatura operatorska
- Monitor minimum 19” (operator dysponuje minimum dwoma widokami obrazu bagażu pod minimum dwoma różnymi kątami)
- Ups pozwalający na bezpieczne zamknięcie systemu w wypadku utraty zasilania
- Projekcję obrazów zagrożenia (TIP) 1000 sztuk z bibliotece przedstawiających, co najmniej 250 rożnych niebezpiecznych przedmiotów, w tym obrazy części składowych niebezpiecznych przedmiotów, przy czym każdy przedmiot powinien być uchwycony w szeregu rożnych położeń
- Wymagana jest coroczna rozbudowa biblioteki obrazów o 100 nowych obrazów przez okres gwarancji
- Logowanie się przez operatorów przy pomocy własnego loginu
- Komunikaty urządzenia w języku polskim
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Znak CE

Stacje operatorskie POZIOM III (bezpieczeństwo)

Wymagana jest minimum jedna stacja.

powinna być wyposażona:

- Klawiatura operatorska
- Monitor minimum 19” (operator dysponuje minimum dwoma widokami obrazu bagażu pod minimum dwoma różnymi kątami)
- Ups pozwalający na bezpieczne zamknięcie systemu w wypadku utraty zasilania
- Projekcję obrazów zagrożenia (TIP) 1000 sztuk z bibliotece przedstawiających, co najmniej 250 rożnych niebezpiecznych przedmiotów, w tym obrazy części składowych niebezpiecznych przedmiotów, przy czym każdy przedmiot powinien być uchwycony w szeregu rożnych położeń
- Wymagana jest coroczna rozbudowa biblioteki obrazów o 100 nowych obrazów przez okres gwarancji
- Logowanie się przez operatorów przy pomocy własnego loginu
- Komunikaty urządzenia w języku polskim
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Znak CE

Stacje Ponownej kontroli POZIOM IV

Wymagana jest minimum 1 stacja z ręcznym czytnikiem kodów kreskowych.

Stacja powinna być wyposażona:

- Klawiatura operatorska
- Monitor minimum 19” (operator dysponuje minimum dwoma widokami obrazu bagażu pod minimum dwoma różnymi kątami)
- Czytnik kodów IATA
- Ups pozwalający na bezpieczne zamknięcie systemu w wypadku utraty zasilania
- Logowanie się przez operatorów przy pomocy własnego loginu
- Komunikaty urządzenia w języku polskim
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Znak CE

Stacje operatorskie (kontrola celna)

Wymagana jest minimum 1 stacja.

Stacja powinna być wyposażona:

- Klawiatura operatorska
- Monitor minimum 19” (operator dysponuje minimum dwoma widokami obrazu bagażu pod minimum dwoma różnymi kątami)
- Ups pozwalający na bezpieczne zamknięcie systemu w wypadku utraty zasilania
- Logowanie się przez operatorów przy pomocy własnego loginu
- Komunikaty urządzenia w języku polskim
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Znak CE

Stacja Ponownej kontroli (kontrola celna)

Wymagana jest minimum 1 stacja.

Stacja powinna być wyposażona:

- Klawiatura operatorska
- Monitor minimum 19” (operator dysponuje minimum dwoma widokami obrazu bagażu pod minimum dwoma różnymi kątami)
- Czytnik kodów IATA
- Ups pozwalający na bezpieczne zamknięcie systemu w wypadku utraty zasilania
- Logowanie się przez operatorów przy pomocy własnego loginu
- Komunikaty urządzenia w języku polskim
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Znak CE

Kontrola bagażu nadwymiarowego

Kontrola bagażu nadwymiarowego odbywa się na dedykowanym urządzeniu rentgenowskim.

Wymogi dotyczące urządzenia:

- Wymiary tunelu 1000mm x 1000mm
- Co najmniej dwa widoki (co najmniej dwa generatory) pod różnymi kątami (widok co najmniej z dołu i boku urządzenia)
- Prędkość taśmociągu: minimum 0,2m/s
- Wysokość taśmociągu dostosowana do wysokości urządzenia
- Penetracja stali: min 35 mm
- Rozdzielczość: min 39 AWG

- Urządzenie wyposażone w konsolę operatorską przystosowana do pracy operatora w pozycji siedzącej.
- Monitor minimum 19” każdy(operator dysponuje minimum dwoma widokami obrazu bagażu pod minimum dwoma różnymi kątami)
- UPS umożliwiający zamkniecie komputera na wypadek awarii zasilania
- Logowanie się przez operatorów przy pomocy własnego loginu
- Funkcja TIP (1000 obrazów)
- Co roku dostarczenie 100 obrazów biblioteki TIP przez okres trwania gwarancji
- Zasilanie 230 Vac/50/60Hz
- Zakres temperatury pracy 5-40°C
- Komunikaty urządzenia w języku polskim
- Interfejs pozwalający na integracje z systemem transportu bagażu
- Interfejs pozwalający na pracę urządzenia w systemie zarządzania urządzeniami RTG
- Walizka testowa
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Znak CE

Kontrola celna (przyloty)

Kontrola bagażu odbywa się na dedykowanym urządzeniu rentgenowskim.

Wymogi dotyczące urządzenia:

- Wymiary tunelu 1000mm x 1000mm
- Jeden widok (jeden generator)
- Prędkość taśmociągu: minimum 0,2m/s
- Wysokość taśmociągu dostosowana do wysokości urządzenia
- Penetracja stali: min 29 mm
- Rozdzielczość: min 36 AWG
- Urządzenie wyposażone w konsolę operatorską przystosowana do pracy operatora w pozycji siedzącej.
- Monitor minimum 19”
- UPS umożliwiający zamkniecie komputera na wypadek awarii zasilania
- Logowanie się przez operatorów przy pomocy własnego loginu
- Zasilanie 230 Vac/50/60Hz
- Zakres temperatury pracy 5-40°C

- Komunikaty urządzenia w języku polskim
- Walizka testowa
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Interfejs pozwalający na integracje z systemem transportu bagażu
- Interfejs pozwalający na pracę urządzenia w systemie zarządzania urządzeniami RTG
- Znak CE

Punkt kontroli bezpieczeństwa pasażerów, VIP, pracowników

(łącznie 4 szt)

Każda linia powinna być wyposażona w urządzenie RTG, podajniki rolkowe, kuwety dla bagażu oraz bramowe wykrywacze metalu.

Wymagania dotyczące urządzenia RTG:

- Wymiary tunelu minimum 600mm x 400mm
- Minimum dwa widoki pod różnymi kątami (minimum dwa generatory)
- Urządzenia mają możliwość kontorli płynów LEDS (min. Standard II, typ C)
- Prędkość taśmociągu min. 0,2 m/s
- penetracja stali: min 35 mm
- Rozdzielczość: min 38 AWG
- UPS – umożliwiający zamkniecie systemy na wypadek awarii zasilania.
- Funkcja TIP (1000 obrazów)
- Co roku dostarczenie 100 obrazów biblioteki TIP w okresie gwarancji
- Konsola operatorska z możliwością pracy operatora w pozycji siedzącej
- Monitor o przekątnej minimum 19” każdy(operator dysponuje minimum dwoma widokami obrazu bagażu pod minimum dwoma różnymi kątami)
- Min. 25 kuwet na linię (20 kuwet klasycznych, 5 kuwet dedykowanych do kontroli płynów)
- Podajniki rolkowe przed urządzeniem o długości 2 metrów
- Podajniki rolkowe za urządzeniem o długości 2 metrów
- stały stół odkładczy
- Walizka STP
- Wszelkie wymagane przez producenta kalibratory i testery
- Zasilanie 230 Vac/50/60Hz
- Zakres temperatury pracy 5-40°C

- Komunikaty urządzenia w języku polskim
- Interfejs pozwalający na pracę urządzenia w systemie zarządzania urządzeniami RTG
- Instrukcja obsługi w języku polskim
- Instrukcja techniczna w języku polskim lub angielskim
- Znak CE

Wytyczne dotyczące bramowego wykrywacza metali (łącznie 4 szt)

- Urządzenie musi spełniać Standard II
- Minimalne wymiary wewnętrzne urządzenia: wys. 2000 mm, szer. 700 mm
- Funkcja random alarm
- Alarm wizualny i dźwiękowy
- Panel pozwalający na zmianę wybranych parametrów
- Oznakowani wizualne nakazujące operatorowi „iść" lub „stać"
- Niezbędne kalibratory wymagane przez producenta
- Niezbędne testery do weryfikacji ustawień bramki (np. noże „opinel", imitacje broni)
- Zasilanie 230 VAC/50/60Hz
- Zakres temperatury pracy 5-40°C
- Instrukcja obsługi w języku polskim
- Interfejs konieczny do pracy w sieci
- Generowanie statystyk
- Znak CE

Urządzenie dedykowane do kontroli płynów LEDS
(min standard II typ B, min standard II typ A)
(1 szt.)

Zamawiający dopuszcza dostarczenie dwu urządzeń (jedno spełniające min standard II typ B, drugie min standard II typ A

Urządzenie musi spełniać następujące wymogi:

- Czas analizy: nie dłuższy niż 15 sekund
- Objętość kontrolowanych płynów: pojemności min od 100ml do 2000ml
- Rodzaje kontrolowanych pojemników: niezależnie od kształtu, koloru (transparentne i nie transparentne), oraz materiału z jakiego są wykonane (szkło, plastik, papier, tetra

pack: płyny w opakowaniach "kartonowych", metal). W przypadku, gdyby któryś z pojemników nie mógł być sprawdzony urządzenie musi jednoznacznie to sygnalizować.

- Alarm wizualny i dźwiękowy
- Komunikaty w języku polskim
- Niezbędne kalibratory wymagane przez producenta
- Zasilanie 230 VAC/50/60Hz
- Zakres temperatury pracy 5-40°C
- Instrukcja obsługi w języku polskim
- Interfejs konieczny do pracy w sieci
- Znak CE

Urządzenia kontroli radiometrycznej

System monitoringu promieniowania jądrowego

System monitoringu promieniowania jądrowego musi zapewniać:

Detekcję i określenie dawki promieniowania jądrowego zarówno elektromagnetycznego jak i korpuskularnego oraz wskazanie automatyczne poprzez alarm przekroczenie określonego poziomu promieniowania.

Możliwości zmiany poziomu alarmowego w zależności od zmian poziomu tła

Rejestrację (archiwizację) wraz z wydrukiem wszystkich stanów alarmowych, które wystąpiły w bagażu rejestrowanym.

System do kontroli obecności materiałów radioaktywnych i jądrowych w bagażu rejestrowanym

Kontrola radiometryczna powinna być oparta na systemie zdalnego sterowania składającego się z następujących elementów:

- Stacjonarnych urządzeń radiometrycznych,
- Komputera nadzorującego prace systemu.

System musi składać się z następujących elementów:

- urządzenia kontrolne gamma-neutronowe (detektory promieniowania) rozmieszczone w strefach objętych nadzorem,
- lokalne sygnalizatory (optyczno-akustyczne) informujące służby pracujące w strefie kontrolnej o powstałym alarmie,
- centralny punkt (sterownik) umożliwiający monitorowanie bieżącego stanu detektorów oraz rejestrację zdarzeń alarmowych,

- system powinien spełniać wymóg zatrzymania systemu taśm na wypadek zasygnalizowania ładunku promieniotwórczego.

Typy stref pomiarowych:

- Punkty kontroli bagażu na odlotach– kolumny pomiarowe będą umieszczone w pobliżu taśmociągów bagażowych lub bezpośrednio nad taśmociągami bagażowymi za punktami kontroli bezpieczeństwa.
- Punkt kontroli bagażu nadwymiarowego na odlotach – kolumny pomiarowe będą umieszczone w pobliżu taśmociągów lub bezpośrednio nad nimi za punktami kontroli bezpieczeństwa.
- Punkty kontroli bagażu na przylotach - kolumny pomiarowe usytuowane przy wjeździe na zewnątrz budynku.

Strefy pomiarowe o wysokości do 2,0 m oraz o szerokościach 1,5 m, 3,0 m oraz 6,0 m będą umieszczone na zewnątrz terminala pasażerskiego.

Stacjonarny monitor promieniowania Gamma – Neutronowego

Wymagania dotyczące głowic Gamma – Neutronowych

- Urządzenie musi posiadać detektor gamma o czułości nie mniejszej niż:
  - 78 (imp/s)/(nSv/h) dla 241Am;
  - 26 (imp/s)/(nSv/h) dla 137 Cs;
- Urządzenie musi posiadać detektor neutronów o czułości nie mniejszej niż 500 zliczeń/cm2/n dla Pu-α-Be;
- Urządzenie musi posiadać detektor ruchu;
- Urządzenie musi posiadać sygnalizator optyczno-akustyczny;
- Urządzenie musi być przystosowane do zasilania z sieci energetycznej o parametrach obowiązujących na terytorium Polski (50-69 Hz, 220-230 V);
- Urządzenie musi pracować w sposób ciągły (24h/dobę) bez konieczności ingerencji ze strony człowieka, w przypadku awarii źródła zasilania sieciowego mieć możliwość przejścia na zasilanie awaryjne z akumulatora;
- Urządzenie musi pracować w warunkach wewnętrznych od 0^0C do +50^0C, w zakresie wilgotności 5-95%;
- Głowica pomiarowa musi posiadać dodatkowe wyjścia przekaźnikowe umożliwiające w przypadku powstania alarmu:
  - podłączenie dodatkowych sygnalizatorów;

    - sterowanie systemem taśmociągów (np. awaryjne zatrzymanie taśmociągu itp.);
- Zalecana odległość głowicy pomiarowej od urządzenia rentgenowskiego bagażu to 3-5m;
- Urządzenie zapewnia dwukierunkową komunikację pomiędzy blokami detekcji a lokalnym kontrolerem, która umożliwia:
    - zdalną kontrolę pracy monitorów;
    - zdalną zmianę nastaw parametrów;
    - wizualizacja danych:
    - podgląd bieżących zliczeń w trybie tekstowym i graficznym;
    - zapis do historii zdarzeń;
    - podgląd parametrów pracy monitora;
    - automatyczny zapis z przebiegu alarmu;
    - automatyczny wydruk raportu ze zdarzenia alarmowego;
    - możliwość wydruku raportu o aktualnym stanie pracy urządzenia.

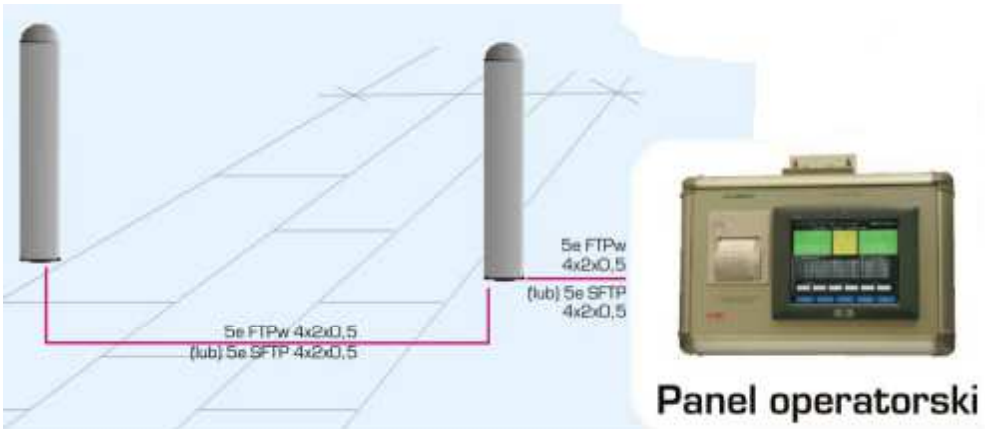
Centralny punkt monitorowania punktów pomiarowych

Niezależnie od zainstalowanych lokalnie sygnalizatorów optyczno-akustycznych oferowany system musi zapewnić:

- możliwość budowy centralnego punktu monitorującego stan pracy punktów pomiarowych oraz rejestrujący powstałe alarmy;
- nadzorowanie pracy bloków detekcji poprzez sieć komputerową;
- prezentacja informacji na mapie synoptycznej obiektu;
- obrazowanie pracy urządzeń;
- odczyt parametrów, jak i zdalne dokonywanie zmian istotnych parametrów detekcyjnych w każdym lokalnym punkcie pomiarowym (funkcja zabezpieczona hasłem);
- rejestrowanie stanów alarmowych i awaryjnych;
- rejestrowanie zmian ustawień stacjonarnych monitorów promieniowania ;
- gromadzenie danych o działaniu systemu;
- automatyczne wykonywanie kopii bazy danych;
- generowanie raportów i zestawień z pracy systemu;
- wydruk alarmów na pojedynczej drukarce dla wszystkich podłączonych punktów pomiarowych (wydruk w kolejności zadziałania punktów pomiarowych wraz z nadawaniem kolejnych numerów). Wydruk zapewnia: ciągłości numeracji powstałych alarmów (niezależnie od punktu pomiarowego) i opis punktu pomiarowego.

Można zastosować równoważne elementy innych producentów niż analizowane w projekcie pod warunkiem zapewnienia nie gorszych parametrów technicznych przywołanych w opisie . Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

W projekcie analizowano stacjonarny monitor promieniowania gamma i neutronowego SMP-M22.



Detekcja:

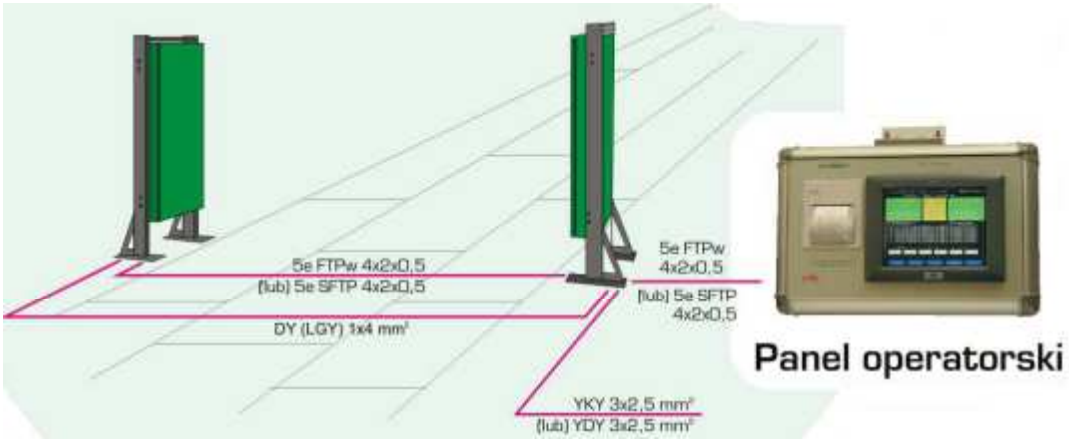
prędkość 5 km/h

Pu-239	1,1g
Pu-239 (4 cm Pb, gamma 1%)	85g
U-235 (HEU)	40g
Cf-252	6000 n/s

neurony He-3śrszer x gł): 1450 x 290 mm

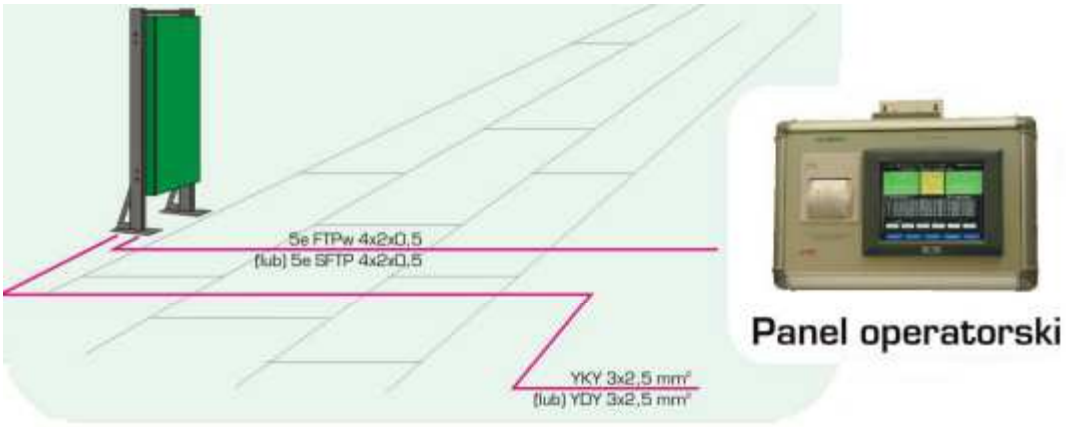
Można zastosować równoważne elementy innych producentów niż analizowane w projekcie pod warunkiem zapewnienia nie gorszych parametrów technicznych opisanych w projekcie. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż

cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.
W projekcie analizowano stacjonarny monitor promieniowania gamma i neutronowego SMP-22 lub równoważny.



Detekcja:
prędkość 8 km/h
Pu-239 1,1g
Pu-239 (4 cm Pb, gamma 1%) 85g
U-235 (HEU) 40g
Cf-252 5000 n/s
neurony He-3
wymiary kolumny pomiarowej (wys x szer x gł): 1650-1800 x 690 x 180 mm

Można zastosować równoważne elementy innych producentów niż analizowane w projekcie pod warunkiem zapewnienia nie gorszych parametrów technicznych opisanych w projekcie.
W projekcie analizowano stacjonarny monitor promieniowania gamma i neutronowego SMP-11 lub równoważny. Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.



Detekcja:

prędkość 5 km/h

Pu-239	1,6g
Pu-239 (4 cm Pb, gamma 1%)	120g
U-235 (HEU)	60g
Cf-252	7000 n/s

neurony He-3

wymiary kolumny pomiarowej (wys x szer x gł): 1650-1800 x 690 x 180 mm

Świadczenia dodatkowe

Dostawca urządzeń zapewni szkolenia dla operatorów urządzeń w ilości niezbędnej dla prawidłowej obsługi w ilości nie mniejszej niż 24 operatorów.

Dostawca urządzeń zapewni szkolenia dla obsługi technicznej urządzeń w ilości niezbędnej dla prawidłowej, podstawowej obsługi technicznej nie wymagającej posiadania autoryzacji producenta do obsługi w ramach gwarancji w ilości nie mniejszej niż 12 pracowników obsługi technicznej.

Zestawienie materiałów BHS

Lp	Opis	Długość [mm]	ilość
A	**Urządzenia kierunek ODLOTY**		
1	Chcekin	3000	4
2	Przenośnik taśmowy lotniskowy	5100	1
3	Przenośnik taśmowy lotniskowy	3000	3
4	Przenośnik taśmowy lotniskowy	4800	1
5	Przenośnik taśmowy lotniskowy	2000	11
6	Przenośnik taśmowy obracany	1300	5
7	Przenośnik taśmowy lotniskowy	2500	3
8	Przenośnik taśmowy lotniskowy	1500	3
9	Diverter poziomy	2500	1
10	Przenośnik rolkowy grawitacyjny	4000	1
11	Przenośnik rolkowy grawitacyjny	1000	2
12	Odbojnice zabezpieczające	8500	1
13	Bramki wysokości		2
14	Roleta listwowa		6
15	Roleta paskowa		4
16	Skaner 360 st.		1
17	Waga najazdowa		1
18	Waga w linii nadgabarytu		1
19	Czytnik kodów IATA na poziom 4		1
B	**Urządzenia kierunek PRZYLOTY**		
20	Przenośnik taśmowy lotniskowy	2000	4
21	Karuzela przylotowa	33000	1
22	Odbojnice zabezpieczające	13000	1
23	Roleta listwowa		2
24	Roleta paskowa		2
25	Bramka wysokości		1

Lp	Opis	Długość [mm]	ilość
C	**Urządzenia: strefa kontroli pasażerów**		
26	Przenośnik rolkowy grawitacyjny	2000	6
27	Przenośnik rolkowy grawitacyjny	1000	4
28	Stół odkładczy	1500	6
29	Barierka	2000	1
d	**System sterowania**		
30	Centralna szafa sterująca ze sterownikiem PLC wraz z oprzyrządowaniem na kierunek ODLOTY		1
31	Centralna szafa sterująca ze sterownikiem PLC wraz z oprzyrządowaniem na kierunek PRZYLOTY		1

Zestawienie materiałów systemów bezpieczeństwa bagażu i pasażerów

Można zastosować równoważne elementy innych producentów niż analizowane w projekcie pod warunkiem zapewnienia nie gorszych parametrów technicznych opisanych w projekcie.

lp	lokalizacja	model	ilość
	bagaż rejestrowany		
1	poziom 1	Dwuwidokowe urządzenie RTG o tunelu min szerokość 1000mm wysokość 800mm	1
2	poziom 2 (kontrola bezpieczeństwa)	stacja analiz	2
3	poziom 3 (kontrola bezpieczeństwa)	stacja analiz	1
4	poziom 4 (kontorla bezpieczeństwa)	stacja ponownej kontroli	1
5	ponad gabaryt	Dwuwidokowe urządzenie RTG o tunelu min szerokość 1000mm wysokość 1000 mm	1
6	serwer	zgodnie z opisem	1

bagaż podręczny

7	kontrola bagażu	dwuwidokowe urządzenie RTG z możliwością kontroli płynów LEDS	4
8	kontrola płynów	urządzenie do kontroli płynów LEDS	1
9	bramowe wykrywacze metali	Bramowy wykrywacz metali WTMD	4

Służba Celna

10	przyloty	jednowidokowe urządzenie RTG o tunelu min szerokość 1000mm wysokość 1000 mm	1
11	Kontrola celna - odloty	stacja analiz	1
12	Kontrola celna - odloty	stacja ponownej kontroli	1

lp	lokalizacja	model	ilość

Radiometria

12	Bramka radiometryczna	W projekcie analizowano SMP-M22. Można zastosować rozwiązanie równoważne.	3
13	Bramka radiometryczna	W projekcie analizowano SMP-M11. Można zastosować rozwiązanie równoważne.	1
14	Bramka radiometryczna	W projekcie analizowano SMP. Można zastosować rozwiązanie równoważne.	1
15	Bramka radiometryczna	W projekcie analizowano SMP-11. Można zastosować rozwiązanie równoważne.	2

Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

Lotniskowe systemy informatyczne

System informatyczny FIS

System informacji lotniczej FIS oparty na centralnej bazie danych i gromadzi, przetwarza i publikuje informacje związane z ruchem lotniczym na lotnisku. System jest wyposażony w moduły operacyjne do wykorzystania przez służby obsługi naziemnej. System współpracuje z systemami informacji wizualnej FIDS i głosowej, oraz z systemem transportu i kontroli bagażu i systemem DCS. Przesył informacji do współpracujących systemów odbywa się automatycznie wg. harmonogramu z centralnej bazy danych i/lub na podstawie wiadomości z systemów zewnętrznych.

Założenia funkcjonalne

System zgodny jest z standardami IATA zatem wszystkie dane prezentowane są zgodnie z tą nomenklaturą.
System jest dostępny w dwóch językach: polskim i angielskim.
System jest oparty o strukturę klient-serwer.
Serwer gromadzi dane w dowolnej bazie danych zgodnej ze standardami ODBC oraz umożliwia równoczesną pracę wielu użytkowników na tych samych zbiorach danych w sposób asynchroniczny/zdarzeniowy.
Zapis danych pochodzących z innych źródeł niż interfejs użytkownika w aplikacji klienta odbywa się za pośrednictwem konfigurowalnych serwisów pozwalających na zbudowanie rozproszonej struktury kolektorów danych.
Do systemów dostarczających dane zewnętrzne należy system przesyłający wiadomości typu B (np.: Sita Sitatex, Arinc Avinet),
Informacje rozgłaszane do/z systemów zintegrowanych z systemem są rozsyłane automatycznie przez serwer w sposób asynchroniczny/zdarzeniowy.
Gromadzone dane wprowadzone z poziomu interfejsu użytkownika lub za pośrednictwem kolektorów danych są automatycznie publikowane do wszystkich połączonych klientów oraz serwisów w sposób asynchroniczny od razu po otrzymaniu i przetworzeniu informacji przez serwer o ile są uprawnieni do otrzymywania danego typu informacji.

Wymagania minimalne dla systemu FIS

System musi posiadać bazę słownikową typów statków powietrznych operujących w lotnictwie cywilnym składającą się z danych:

- Kod IATA,
- KOD ICAO,
- Nazwa typu statku powietrznego,
- Wake category,
- Typical first class configuration,
- Typical second class configuration,
- Cargo,
- Maximum fuel capacity,
- Maximum takeoff weight,
- Maximum range,
- Typical cruise speed,
- Rozmiary: wing span, wing span with winglets, overall length, tail height,
- interior cabin width,
- Sylwetki samolotów.

System musi posiadać bazę słownikową rejestracji składającą się z danych:

- Rejestracja statku powietrznego,
- Typ statku powietrznego,
- Linia lotnicza.

System musi posiadać bazę słownikową linii lotniczych składającą się z danych:

- Kod IATA,
- Kod ICAO,
- Nazwa linii lotniczej,
- Kraj,
- Informacja czy linia jest typu lowcost.

System musi posiadać bazę słownikową portów lotniczych składającą się z danych:

- Kod IATA,
- Kod ICAO,
- Nazwa portu,
- Kraj,
- Informacja czy port jest w strefie Schengen czy nie.

Rozwiązanie powinno składać się z modułów umożliwiających:

- Układanie, edycję, podgląd oraz publikacja rozkładu rejsów,
- Podgląd depesz MVT, LDM, PSM, PTM, SLS itp.,
- Automatyczne wiązanie depeszy przychodzącej oraz wychodzącej z odpowiadającym mu rejsem wprowadzonym do rozkład rejsów,
- Interpretacja depesz polegająca na wydzieleniu pól z depeszy o specyficznym znaczeniu oraz prezentacja tych informacji na interfejsie użytkownika,
- Edycję i rozszerzanie bazy danych takich jak: baza portów lotniczych,
- baza statków powietrznych, baza linii lotniczych wraz z oznaczeniami IATA oraz ICAO,
- Zarządzenie użytkownikami systemu oraz ich uprawnieniami pozwalającymi na profilowanie uprawnień do poszczególnych modułów systemu takich jak: dostęp, podgląd, edycja, dodawanie nowych danych oraz ich usuwanie,
- Dostęp do danych operacyjnych pozwalających na szybki dostęp do informacji takich jak: nadchodzące rejsy przylotowe oraz odlotowe,
- opóźnienia, liczba pasażerów odczytana z widomości MVT lub LDM, liczba asażerów z bookingu , godzina przylotu, godzina wylotu,
- Prezentacja danych czasowych w postaci wykresów Gantta ułatwiających interpretację danych czasowych oraz w postaci tabeli,
- Możliwość szybkiej filtracji danych prezentowanych w systemie po wybranych filtrach czasowych, numerów rejsów, kodów opóźnień oraz innych filtrów,
- Możliwość wydruku danych prezentowanych w dowolnym module systemu wraz z możliwością ich eksportu do pliku CSV, HTML, XLS itp.,
- Możliwość planowania stanowisk postojowych dla statków powietrznych,
- Możliwość generowania raportów oraz statystyk takich jak:
    - Liczba rejsów wraz z podziałem na ich typy (regularny, czarterowy, cargo, specjalny) w określonym przedziale czasu z możliwością filtracji po: rejsach przylotowych, odlotowych, liniach lotniczych, destylacjach, typach statków powietrznych, terminalach, itp.,
    - Statystyki opóźnień wraz z możliwością filtracji po: rejsach przylotowych, odlotowych, liniach lotniczych, destylacjach, typach statków powietrznych, terminalach, itp.,
    - Statystyki liczby podróżnych wraz z możliwością filtracji po: rejsach przylotowych, odlotowych, liniach lotniczych, destynacjach, typach statków powietrznych, terminalach, touroperatorach, itp.,

- Możliwość zarządzania zasobami ludzkimi oraz sprzętowymi (w aspekcie operacyjnym portu lotniczego) w module planowania z automatycznym przypisywaniem do wykonywania określonych czynności lub funkcji zgodnie z uprawnieniami, szkoleniami lub przeznaczeniem przy określonym rejsie,
- Możliwość wystawienia noty handlingowej będącej potwierdzeniem wykonania usług,
- Możliwość konfigurowania listy usług wykonywanych dla danego przewoźnika oraz typu statku powietrznego celem Możliwość wystawiania dokumentu Service rendered,
- Możliwość wystawienia dokumentu Graoud Handling Note
- Możliwość pracy w środowisku wielomonitorowym pozwalając na pracę z
- wieloma modułami umieszczonymi na różnych ekranach.
- System musi być zgodny z Polskim prawodawstwem a w szczególności z obowiązującymi przepisami prawa pracy na dzień odbioru systemu
- System musi umożliwić dostęp do danych służbom „mundurowym" a szczególności : SOL, SG, UC
- System musi mieć możliwość dostępu do danych na pokładzie statku powietrznego jak i w obrębie terminala pasażerskiego
- Powinien mieć możliwość współpracy z posiadanym systemem do fakturowania Symfonia Forte.
- Powinien musi mieć możliwość współpracy z posiadanym systemem Informacji wizualnej dla podróżnych
- System powinien mieć możliwość integracji z systemem łączności cyfrowej TETRA

Możliwość przeglądania wszystkich depesz

Możliwość filtrowania depesz po treści.

Możliwość filtrowania depesz po dowolnym znaku.

Planowanie rozkładu rejsów

Od modułu planowania rejsów wymaga się możliwości wprowadzania do siatki rozkładu rejsów zarówno cyklicznych jak i pojedynczych. Rejs powinien być powiązany z informacjami takimi jak:

- Typ rejsu – regularny, charterowy, specjalny, cargo itp.,
- Numer rejsu przylotowy oraz odlotowy z automatyczną weryfikacją poprawności linii lotniczej,
- Typ statku powietrznego zgodnie z kodami IATA lub ICAO,
- Rejestracja statku powietrznego,
- Trasę przelotu (z, przez, baza, przez, do) zgodnie z oznaczeniami IATA lub ICAO,

- Dodatkowe informacje o rejsie z postaci pola tekstowego,
- Informacja o przylocie lub odlocie na pusto (ferry-in, ferry-out),
- Datę oraz czas przylotu,
- Datę oraz czas odlotu,
- Datę oraz czas odloty ze stacji wylotu,
- Datę oraz czas przylotu do stacji docelowej,
- Możliwość wyboru czasu lokalnego lub czasu UTC w maskach służących do wprowadzania danych o rozkładzie rejsów,
- Maska rejsu rekurencyjnego pozwalająca na wybór dni tygodnia operowania danego rejsu,
- Informacje o bookingu czyli planowanej liczbie pasażerów,
- Informację o numerze radiotelefonu, telefonu,
- Informację o numerze Gate,
- Informację o pozycji postojowej dla statku powietrznego.
- Wizualizacja rotacji statków powietrznych na płycie lotniska w sposób
- graficzny za pomocą linii łączących rotujące statki powietrzne na płycie lotniska.
- Dowolnego ułożenia kolejności kolumn,
- Sortowania po jednej lub wielu kolumnach,
- Włączanie lub wyłącznie widoku wybranej kolumny,
- Filtrowania po dowolnej kolumnie,
- Wydruku danych bieżącego widoku,
- Publikacji email danych bieżącego widoku,
- Eksport danych do schowka bieżącego widoku,
- Wzorzec tygodniowy operowania rejsu.

Moduł powinien wykrywać możliwe konflikty z numerami rejsów już wprowadzonymi do systemu operujących w tych samych dniach co nowe rejsy lub mieszczące się w określonym odstępie czasowym.

Wszystkie tabele powinny być konfigurowalne pozwalając na wybór kolejności kolumn, sortowanie po wielu kolumnach, filtrowanie zawartości. Powinna istnieć także możliwość publikacji danych bezpośrednio z modułu planowania rozkładu rejsów w postaci wiadomości e-mail z załączonym dokumentem prezentującym dane o rozkładzie rejsów do wybranej, konfigurowalnej listy odbiorców. Rozwiązanie publikujące dane w postaci wydruku, poczty e-mail, eksportu danych do schowka powinno posługiwać się zasadą WYSIWYG. Zatem publikowane powinny być tylko te dane które zostały odfiltrowane z zachowaniem sortowania.

Integracja z systemem przesyłającym wiadomości typu B

Rozwiązanie powinno być zintegrowane ze środowiskiem przesyłającym wiadomości typu B pozwalając na automatyczny, ciągły import danych zawartych w depeszach różnego typu. Depesze przychodzące oraz wychodzące powinny być wiązane z rejsem dodanym w module planowania rozkładu oraz zdekodowane, które będą wykorzystane w innych częściach systemu. Wymagana jest zdolność zapisywania oraz interpretowania depesz typu: MVT, LDM, SLS, ASM, CPM. System ma zapewnić szybki i łatwy dostęp do kolekcji depesz każdego typu w osobnym module, wraz z możliwością wydruku listy oraz filtracji po wybranych kolumnach takich jak: numer rejsu, kod opóźnienia, przewoźnik, czas odebrania depeszy itp.
Na etapie wdrożenia należy zapewnić integracje za równo systemami operatora
SITA jak i ARINC

Tabele

Moduł powinien posiadać tabele:

- Kontener główny, będący zbiorem wszystkich wiadomości wysłanych na określone adresy odbiorców, gdzie lista adresów powinna być konfigurowalna na serwerze odbierającym dane, zapisującym je w bazie AODB, oraz rozsyłającym nowe wiadomości do zalogowanych użytkowników posiadających prawa do odczytu tych wiadomości,
- Kontener z wiadomościami MVT, będący zbiorem wszystkich wiadomości ruchowych,
- Kontener z wiadomościami LDM, będący zbiorem wszystkich wiadomości Load Messeges,
- Kontener z wiadomościami SLS, będący zbiorem wszystkich wiadomości SLS,
- Kontener z wiadomościami ASM, będący zbiorem wszystkich wiadomości ASM,
- Kontener z wiadomościami CMP, będący zbiorem wszystkich wiadomości SMP.
- Każda z tabel powinna być tabelą pozwalającą na dowolne ułożenie kolejności kolumn, sortowanie po wielu kolumnach oraz filtrowanie danych w wielu kolumnach, pozwalając na tworzenie złożonych filtrów. Wszystkie ustawienia widoku powinny być zapamiętywane i odtwarzane przy ponownym uruchomieniu platformy. Praca z danymi w tabelach powinna przypominać pracę z dokumentami Excela, to znaczy nawigacja po polach tabeli powinna następować za pomocą kursorów klawiatury.

Postać tabelaryczna kontenera głównego wiadomości powinna zawierać takie dane jak:

- Czas odebrania lub wysłania wiadomości,
- Zawartość oryginalnej wiadomości,
- Linia lotnicza,
- Priorytet wiadomości,

- Adres nadawcy,
- Lista adresów odbiorców,
- Temat wiadomości,
- Typ wiadomości (MVT, LDM, PSM, PTM, SLS i inne),
- Informacja czy jest to wiadomość przychodząca czy wychodząca

Dane, które powinny być interpretowane z depesz MVT to:

- Numer rejsu
- Dzień operowania
- Rejestracja statku powietrznego
- Oznaczenie IATA portu wysyłającego informację
- Czasy: touchdown, chocks on block, off-block, take off, estimated time
- of arrival, estimated time of departure, next information
- Oznacznie IATA portu do którego skierowana jest wiadomość
- Dodatkowe informacje
- Kody opóźnień
- Pax

Dane, które powinny być interpretowane z depesz LDM to

- Numer rejsu
- Dzień operowania
- Rejestracja statku powietrznego
- Wersja statku powietrznego
- Załoga
- Oznaczenie IATA portu do którego skierowana jest wiadomość
- Liczba pasażerów z wydzieleniem liczby infantów
- Liczba pasażerów na klasę
- Poczta, cargo

Moduł operacyjny

Część operacyjna systemu powinna zawierać informacje o nadchodzących rejsach przylotowych oraz odlotowych, prezentowanych w postaci wykresu Gantta oraz tabeli w określonym przedziale czasowym ‘do przodu’ lub w wybranym z kalendarza dniu lub okresie czasu. Dane przylotowe oraz wylotowe powinny być prezentowane na osobnych tabelach i wykresach Gantta.

Postać tabelaryczna operacji przylotowych powinna zawierać takie dane jak:

- Numer rejsu,

- Data oraz czas przylotu,
- Czas ATA,
- Czas ETA,
- Trasa przelotu,
- Typ statku powietrznego,
- Rejestracja statku powietrznego,
- Numer pozycji postojowej statku powietrznego na płycie lotniska,
- Numer radiotelefonu, telefonu,
- Imię i nazwisko Ramp Agenta,
- Kody opóźnień zaimportowane z depesz MVT,
- Liczba pasażerów pobrana z depesz LDM,
- Cargo pobrana z depesz LDM,
- Załoga pobrana z depesz LDM,
- Poczta pobrana z depesz LDM,
- Pole dodatkowych informacji tekstowych.

Postać tabelaryczna operacji przylotowych powinna dawać możliwość:

- Dowolnego ułożenia kolejności kolumn,
- Sortowania po jednej lub wielu kolumnach,
- Włączanie lub wyłącznie widoku wybranej kolumny,
- Filtrowania po dowolnej kolumnie,
- Eksport danych do schowka bieżącego widoku.
- Rozróżniania graficznego rejsów o różnym statusie:
    - Status nieokreślony, dla rejsów o nieznanych danych ETA, ATA, DL, CANCEL,
    - Status rejsu opóźnionego w przypadku gdy różnica między czasem ATA a ETA jest większa niż określona wartość konfigurowana w ustawieniach programu,
    - Status rejsu na prostej,
    - Status rejsu odwołanego,
    - Status rejsu wylądował.
- Wyświetlania podsumowania z liczby operacji przewoźników w postaci tabeli zawierającej:
    - Nazwę linii lotniczej wraz z kodem IATA,
    - Liczba wszystkich operacji,

- Liczba operacja dla każdego typu rejsu (regularny, charter, cargo, special, symulowany). wraz z numerem rejestracyjnym statku powietrznego, kodem opóźnienia, liczbą pasażerów.

Informacje te powinny zostać pobrane z wiadomości typu B. Dodatkowo celem ułatwienia interpretacji ekranu powinno nastąpić rozróżnienie graficzne rejsów o statusie nieznanym, opóźnione, odwołane, wylądowały, wystartowały. Każdemu rejsowi z poziomu ekranu operacyjnego powinno dać się przypisać status ‘wylądował’, ‘wystartował’, ‘na prostej’ lub ‘odwołany’. Nadanie statusu ‘wylądował’ powinno skutkować wyświetleniem dodatkowej informacji zawierającej numer rejsu oraz czas jego lądowania lub startu. Wszystkie dane dodatkowe związane z rejsem jak: numery stanowisk postojowych, numery otwartych stanowisk check-in, numery otwartych gate’ów, lista osób przypisanych do obsługi rejsu, lista sprzętu przypisanego do obsługi rejsu, lista depesz lotniczych każdego interpretowanego typu, powinna być dostępna w osobnym oknie wraz z możliwością edycji i dokonywania zmian. Ponadto w module tym powinna istnieć możliwość przeglądu operacyjnych danych historycznych wraz z możliwością filtracji po: numerach rejsów, liniach lotniczych, kodach opóźnień, destynacjach
Moduł operacyjny powinien posiadać możliwość wydruku raportów o spodziewanych operacjach, raportu dziennego z zachowaniem danych o rotacji statków na płycie, raportu z blokingu.
Tabele modułu operacyjnego powinny być konfigurowalne pozwalając na dowolne ułożenie kolejności kolumn, sortowanie po wielu kolumnach oraz filtrowanie danych w wielu kolumnach, pozwalając na tworzenie złożonych filtrów. Wszystkie ustawienia widoku powinny być zapamiętywane i odtwarzane przy ponownym uruchomieniu platformy. Praca z danymi w tabelach powinna przypominać pracę z dokumentami Excela, to znaczy nawigacja po polach tabeli powinna następować za pomocą kursorów klawiatury

Moduł danych słownikowych

Moduł ten powinien pozwalać na tworzenie własnych baz typów statków powietrznych, statków powietrznych, linii lotniczych, portów lotniczych. Wszystkie dane wprowadzone w moduł słownikowy powinny opierać się o standard oznaczeń IATA oraz ICAO. Dodatkowym atutem będzie możliwość prowadzenia szczegółowych danych o statkach powietrznych zawierających takie informacje jak:

- Wake category,
- Typical first class configuration,
- Typical second class configuration,
- Cargo,

- Maximum fuel capacity,
- Maximum takeoff weight,
- Maximum range,
- Typical cruise speed,
    - Rozmiary: wing span, wing span with winglets, overall length, tail height, interior cabin width.

Zarządzania Personelem operacyjnym

Moduł ten powinien spełniać następujące kryteria :

- ograniczenia związane z prawem pracy, np. zapewnienie odpowiednich przerw szczególnie po zmianach nocnych, minimalna i maksymalna dopuszczalna liczba godzin pracy na jednej zmianie.
- zapewnienie właściwej liczby osób obsługi, zgodnie z umowami podpisanymi z liniami lotniczymi).
- zapewnienie odpowiedniej liczby osób z kadry kierowniczej, przebywających na lotnisku.
- zbierać dane razem ze wszystkimi wymaganiami i ograniczeniami. Każdej grupie lub, jeśli to jest wymagane, pojedynczemu pracownikowi, powinien umożliwić przypisanie :
    - rodzaje i liczbę zmian w miesiącu lub w tygodniu,
    - maksymalną/minimalną liczbę godzin pracy na miesiąc
    - typ zatrudnienia

System powinien umożliwić każdej grupie przypisanie poszczególnych rejsów lub całych linii lotniczych. Każdy pracownik może należeć do kilku grup, ze względu na odpowiednie szkolenia.

- Optymalizować grafik , tak aby był korzystny zarówno dla lotniska, jak i dla pracownika, uwzględniając jego preferencje, jak np.:
    - możliwość ustalenia dni wolnych, lub zmian w pewne dni,
    - możliwość tych samych godzin pracy z wybranymi osobami.
- Wspomóc ręczne planowanie, pozwalając osobie planującej lub poszczególnym kierownikom na dokonywanie korekt. Automatycznie sygnalizować naruszenie ograniczeń oraz pozwolić na podmianę godzin przyjść i przydziałów dwóch pracowników o tych samych kwalifikacjach.
- Przygotować plan, który może zostać wydrukowany i przekazany każdemu pracownikowi.

Moduł rampy

Moduł rampy powinien pozwalać na tworzenie dokumentów GHN będących potwierdzeniem wykonania usług zgodnie z umową, oraz zawierać mechanizmy pozwalające na automatyczne importowanie listy usług z bazy umów handlingowych. Lista serwisów powinna być konfigurowalna i pozwalać na dowolną zmianę każdej z usług. Na podstawie listy usług system powinien umożliwiać tworzenie dowolnej umowy handlingowej powiązanej z linią lotniczą oraz typem statku powietrznego.

Moduł rampy powinien być tak skonstruowany by pozwalał na:

- Zarządzanie wszystkimi dokumentami przez osobę odpowiedzialną za weryfikację poprawności wykonania usług,
- Przypisywanie osób odpowiedzialnych za wykonanie usług przy operacji wylotowej lub przylotowej,
- Przeglądanie listy rejsów, które zostały przypisane do agenta,
- Modyfikację stanu wykonania usług: przypisany, obsługa rozpoczęta, obsługa zakończona, dokument odrzucony do poprawy, dokument zatwierdzony,
- Drukowanie dokumentów w określonym formacie dostarczonym przez dział obsługi naziemnej.

Dane na dokumencie końcowym, potwierdzającym wykonanie usług powinny zawierać:

- Nazwa portu lotniczego,
- Data i czas wystawienia dokumentu,
- Nazwa lini lotniczej,
- Numer rejsu przylotowego lub/i wylotowego,
- Trasa przelotu,
- Metoda płatności,
- Typ statku powietrznego,
- MTOW,
- Imię i nazwisko kapitana,
- Załoga,
- Numery rejestracyjne statku powietrznego operacji przylotu i wylotu, jeśli są różne,
- Rzeczywistą godzinę przylotu,
- Rzeczywistą godzinę wylotu,
- Kody opóźnień,
- Opis przyczyn opóźnienia,
- Informację o przylocie lub wylocie na pusto,

- Informację o rejsie przekierowanym,
- Informację o odwołaniu operacji,
- Listę wykonanych serwisów wraz z informacjami szczegółowymi jak:
    - Liczba pasażerów przylatujących,
    - Liczba pasażerów wylatujących,
    - Liczba pasażerów tranzytowych,
    - Bagaż przylatujący i wylatujący,
    - Poczta przylatująca i wylatująca,
    - Cargo przylatujące i wylatujące,
    - Inne dane szczegółowe wykonanych serwisów zgodnie z listą szablonów serwisów,
    - Status wykonania usługi,
    - Dodatkowe komentarze do każdej wykonanej usługi.

System powinien zapisywać czas rozpoczęcia i zakończenia obsługi statku powietrznego, oraz osobno czas rozpoczęcia i zakończenia wykonania każdej z usług. System powinien posiadać możliwość pracy na urządzeniach mobilnych z ekranem dotykowym. Tak samo jak w innych modułach dane przedstawione tabelarycznie powinny dawać możliwość:

- Dowolnego ułożenia kolejności kolumn,
- Sortowania po jednej lub wielu kolumnach,
- Włączanie lub wyłącznie widoku wybranej kolumny,
- Filtrowania po dowolnej kolumnie,
- Eksport danych do schowka bieżącego widoku,
- Wybranie dowolnej daty z kalendarza celem przeglądu danych historycznych.

Wymagania i specyfikacje sprzętowe

Stacje robocze FIS wraz z konfiguracją i oprogramowaniem FIS

Wymagania minimalne stacji roboczych:

- monitor min. 22"
- jednostka PC o minimalnych parametrach:
- procesor min. 3,14 GHz
- pamięć RAM min. 3,5 GB
- dysk HDD 250 GB lub większy

- karta sieciowa 10/100/1000 Mbit/s
- system operacyjny Windows 7 Ultimate lub wyższy
- gniazda odpowiednie do stosowanych urządzeń peryferyjnych
- klawiatura i mysz

Mobilne stacje robocze FIS wraz z konfiguracją i oprogramowaniem FIS

Wymagania minimalne mobilnych stacji roboczych:

- Klasa procesora: i3-2330M;
- Prędkość procesora: 2,2 GHz;
- Częstotliwość szyny QPI/DMI: 5 GT/s;
- Pojemność pamięci podręcznej: 3 MB;
- Technologia Hyperthreading: Tak;
- Pojemność dysku (HDD): 320 GB;
- Zainstalowana pamięć: 2048 MB;
- Przekątna ekranu LCD: 10,4 cali; Typ ekranu: TFT HD [LED];
- Bezprzewodowa karta sieciowa: Tak;
- Zainstalowany system: Microsoft OEM Windows 7 Ultimate SP1 64 bit, Polish, 1pk, DVD,

Serwery systemu FIS wraz oprogramowaniem

System będzie zainstalowany na dwóch identycznych serwerach rack 19” o następujących parametrach minimalnych:

- Procesor min: INTEL XEON X3450 PROCESSOR (2.66GHZ, 4C)
- Pamięć ram: 8GB (2X4GB DUAL RANK LV UDIMMS)
- Dyski twarde:2x 146GB SAS 6GBPS 10K 2.5" HYBRID HD pracujące w układzie RAID1.
- Napęd DVD:16X DVD+/-RW DRIVE SATA.
- Zasilacze: 2x REDUNDANT POWER SUPPLY (2 PSU) 400W .
- Zintegrowany kontroler zdalnego dostępu
- System operacyjny: SUSE LINUX ENTERPRISE SERVER 11 SP1

Zestawienie materiałów i licencji

Lp	Typ	Nazwa	Ilość
1	FIS	Licencja FIS zawierająca licencje na 10 stanowisk, wraz z instalacją i wdrożeniem	1
2	Tablet	Tablet PC, 10.4", HDD, BT, HSUPA, Win XPPro wraz ze stacją dokującą b równoważny	1
3	Serwer	zgodny z opisem	2
4	Komputer	zgodny z opisem	10
5	Monitor	zgodny z opisem	11
6	Nas	zgodny z opisem	1
7	Oprogramowanie	program antywirusowy Nod 32 AV lub równoważny	13
8	KVM	Konsola Monitorowa 19" Rack lub równoważna	1

Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

System informatyczny służący do zapewnienia informacji wizualnej dla pasażerów FIDS

Oprogramowanie systemu FIDS

Oprogramowanie systemu FIDS w połączeniu ze sprzętem umożliwia wyświetlanie żądanych informacji o lotach w połączeniu z plikami multimedialnymi, zawierającymi treści dotyczące bezpieczeństwa, przepisów, organizacji lotniska a także reklamy.

Oprogramowanie FIDS zawiera:

- Standardowe listy multimedialne,
- Standardowe wzory modułów do wyświetlania,
- Możliwość obsługi wielojęzycznej w powiązaniu z miejscem docelowym lotu,
- Możliwość wyświetlania reklam rozłożonych na wielu monitorach z ich synchronizacją czasową tzw. reklama przebiegająca przez wiele monitorów,
- Możliwość przydziału monitorów do grup wspólnie wyświetlających informacje lub reklamy,
- Możliwość wyświetlania plików multimedialnych (reklamy) i informacji jednocześnie, współdzielnie na jednym monitorze
- Możliwość zarządzania monitorami oraz treściami ze stanowiska administracyjnego.

Funkcjonalności systemu FIDS

Przez FIDS rozumie się system prezentujący dane dotyczące operacji lotniskowych.

- System FIDS ma być oparty na bazie danych systemu FIS, która jest baza nadrzędną. Centralna baza danych systemu FIDS zapewni możliwość tworzenia, zapisywania i usuwania danych z zastosowaniem zaprogramowanych własnych procesów selekcji.
- W systemie FIDS muszą znajdować się co najmniej dwa serwery (główny i zapasowy). Baza danych znajdująca się na serwerze zapasowym musi być zsynchronizowana z bazą znajdującą się na serwerze głównym. W przypadku awarii serwera głównego musi nastąpić automatyczne przełączenie systemu na serwer zapasowy w sposób niezauważalny dla stacji klienckich. Serwery muszą posiadać własne zasilanie awaryjne.
- Umożliwi prezentację, między innymi w pomieszczeniach ogólno dostępnych tj.: hal główny, restauracje, check-in, parking, w strefach - kontrolowanego dostępu (strefa przylotów), zastrzeżonej i krytycznych częściach strefy zastrzeżonej (bagażownia, sortownia bagażu, strefa odlotów, punkty kontroli bezpieczeństwa, pomieszczenia dla

pracowników), na dowolnym dostępnym typie wyświetlacza następujących typów informacji:

a) dane o lotach aktualizowane na bieżąco w czasie rzeczywistym, z wykorzystaniem technologii aktywnej aktualizacji danych (technologia rozgłaszania) zapewniając minimum:
   - rozkład – przyloty
     - czas przylotu,
     - logo/nazwa przewoźnika,
     - miasto - skąd przylatuje samolot,
     - oczekiwany czas przylotu,
     - numer rejsu,
     - status lotu (opóźniony, wylądował, kołuje, odwołany)
     - inne uwagi.
   - rozkład – odloty
     - czas odlotu,
     - logo/nazwa przewoźnika,
     - miasto - dokąd odlatuje samolot,
     - oczekiwany czas odlotu,
     - numer rejsu,
     - status lotu (opóźniony, kołuje, odwołany)
     - inne uwagi.
   - odprawy (check-in),
     - rodzaj check-in,
     - czas odlotu,
     - logo/nazwa przewoźnika,
     - miasto - dokąd odlatuje samolot,
     - oczekiwany czas odlotu,
     - numer rejsu,
     - inne uwagi.
   - boarding – gate,
     - czas odlotu,
     - logo/nazwa przewoźnika,
     - miasto - dokąd odlatuje samolot,

        - oczekiwany czas odlotu,
        - numer rejsu,
        - inne uwagi.
    - zestawienie bieżących gate-ów układ tabelaryczny ,
        - czas odlotu,
        - logo/nazwa przewoźnika,
        - miasto - dokąd odlatuje samolot,
        - oczekiwany czas odlotu,
    - bagaże,
        - logo/nazwa przewoźnika,
        - miasto - skąd przylatuje samolot,
        - numer rejsu,
        - pierwszy bagaż/ostatni bagaż
    - inne informacje techniczne

b) Sposób prezentacji informacji
    - bieżące – przyloty,
    - bieżące – odloty,
    - rozkład i bieżące – przyloty i odloty razem lub w sposób naprzemienny na jednym monitorze,
    - check-in,
    - boarding – gate,
    - zestawienie bieżących gate-ów układ tabelaryczny,

c) dane o charakterze multimedialnym
    - loga przewoźników,
    - zdjęcia,
    - filmy,
    - informacje dla podróżnych,
    - komunikaty specjalne,
    - instrukcje bezpieczeństwa,
    - wygaszacze ekranu,
    - reklamy,

d) Reklamy w układzie jednomonitorowym

- Zapewni strefowe wyświetlanie informacji tekstowych i multimedialnych - wyświetlanie na całości ekranu, jego dowolnej części w dedykowanym oknie lub w postaci przewijanego paska

e) Reklamy w układzie wielomonitorowym,
   - Równoczesna prezentacja treści reklamy multimedialnej na wielu monitorach równocześnie (synchronizowane czasowo),
   - Prezentacja reklam przebiegających pomiędzy monitorami (synchronizacja czasowa wyświetlania)
   - Prezentacje multimedialne prezentowane na wielu monitorach równocześnie z różnymi treściami, ale synchronizowane czasowo.

- Zapewni możliwość pełnej konfigurowalności wyglądu (np. prezentację danych o kilku lotach naprzemiennie lub w tabeli) i umożliwi pełną zarządzalność wyglądu prezentowanych danych (kolory, czcionki, rozmieszczenie informacji, wielkości elementów) z wykorzystaniem narzędzia WYSIWYG.
- Pozwoli na wyświetlanie informacji w wielu językach na różnych wyświetlaczach, w dowolnych czcionkach i stylach (UTF8). Umożliwi prezentację danych w kilku językach na tym samym wyświetlaczu osobno dla każdej linii (umożliwi to np. prezentację danego komunikatu w danej linii zmiennie w języku polskim i angielskim, z możliwością języka miejsca docelowego).
- Pozwoli na dowolne wykorzystanie monitorów podłączonych do systemu w zakresie wszelkich możliwych informacji i danych zarządzanych przez system (oznacza to, że każdy wyświetlacz z osobna lub w grupach mogą wyświetlać każde dowolne informacje).
- Pozwoli na automatyczny dobór informacji multimedialnej, na podstawie kontekstu, (context sensitive information), który tworzy informacja dotycząca konkretnej operacji lotniczej (informacja o miejscu przeznaczenia, pogoda, informacja turystyczna, reklamy). Informacje muszą być prezentowane zgodnie z przepisami IATA.
- Zapewni możliwość dynamicznej i inteligentnej zmiany informacji (np. w przypadku zmiany gate'u informacja pojawia się automatycznie tylko w odpowiednich miejscach by dotrzeć do konkretnej grupy pasażerów). Pozwoli na wyświetlanie informacji w wielu językach na rożnych wyświetlaczach.
- Umożliwi personelowi na stanowiskach check-inow i w gate`ach dodawanie/edycję komunikatów na bieżąco po zainstalowaniu dodatkowych stacji roboczych.

- Umożliwi każdemu użytkownikowi systemu edycję oraz dodawanie nowych danych w zakresie jego autoryzacji z dowolnego miejsca w porcie.
- Pozwoli na aktualizowanie informacji na wszystkich wyświetlaczach z wykorzystaniem technologii aktywnej aktualizacji danych (technologia rozgłaszania) w czasie nie dłuższym niż 1 sekunda od momentu przesłania jej do systemu.
- Umożliwi przesyłanie danych na stronę internetową portu oraz tworzenie własnych stron internetowych w formacie HTML a także wysyłanie wiadomości w formacie XML.
- System umożliwi zdalną obsługę (parametry fizyczne oraz wyświetlane dane) każdego monitora indywidualnie, ze stacji roboczych. Wybór monitora odbywać się będzie z listy lub/i mapy rzutu terminala z naniesioną lokalizacją monitorów. Użytkownik będzie mógł dowolnie edytować mapy, aktualizować rzuty terminala, dodawać usuwać przenosić poszczególne monitory.
- System umożliwi dokonywanie zmian ustawień i konfigurację monitorów, dodawanie nowych monitorów i stacji roboczych „online" – bez potrzeby zamykania i restartowania całego lub części systemu w celu wprowadzenia i zapisania zmian konfiguracji.
- System umożliwi podgląd oraz wykonanie zrzutu grafiki ekranu z dowolnie wybranego monitora w czasie rzeczywistym, oraz będzie posiadał funkcję podglądu statusu wszystkich monitorów w systemie.
- W przypadku awarii systemu FIS system FIDS będzie w stanie przejąć jego zadania w zakresie wyświetlania informacji pasażerskiej. W związku z tym będzie posiadał funkcjonalność tworzenia dziennych rozkładów lotów na podstawie własnej bazy danych oraz będzie posiadał własny interfejs graficzny do obsługi bazy danych o lotach wraz ze wszystkimi możliwościami ustawień.

Funkcjonalności dodatkowe i współdziałanie z innymi systemami

System FIDS zagwarantuje na dzień składania oferty możliwość jego rozbudowy o następujące moduły dodatkowe których instalacja i uruchomienie będzie należeć do odrębnego zadania:

- Moduł obsługujący kierowanie informacji do personelu oraz administratora przez urządzenia mobilne (smartphone) po sieci wewnętrznej lub TCP/IP
- Moduł IVR Interactive Voice Response pozwalający na automatyczne kierowanie informacji do pasażerów drogą telefoniczną

- Moduł SMS pozwalający na automatyczne wysyłanie wiadomości SMS do pasażerów z powiadomieniem o zmianach statusu ich lotu generowanych na podstawie danych aktualizowanych w FIDS
- Interfejs do innych urządzeń wyświetlających (np. Citylighty, tablice reklamowe, itp.) umożliwiający zarządzenie treścią wyświetlaną na tych urządzeniach tak jak na monitorach LCD
- Interfejs do BHS (przyloty lub/i odloty) umożliwiający automatyczne wyświetlanie informacji o przydzielonych karuzelach lub zrzutniach oraz przekazujący dane rozkładowe do SAC
- Moduł BMID umożliwiający automatyczne sygnalizowanie pierwszego i ostatniego bagażu oraz zajętości karuzel bagażowych z pozycji rozładunku bagażu

Aplikacja umożliwiająca automatyczne i samoczynne wyłączanie monitorów w okresie braku operacji lotniczych i ich dynamiczne i automatyczne włączanie w momencie pojawienia się lotu (rozkładowe, opóźnienia, nowe loty) z uwzględnieniem własnych konfiguracji czasów włączania i wyłączania monitorów.

Wymagania standardów

System FIDS musi być zgodny ze standardami IATA, wszystkie dane prezentowane muszą być zgodnie z nomenklaturą IATA.

Składniki systemu

Zaprojektowany system składa się co z następujących elementów:

- Monitory LCD lub LED 22’ ze zintegrowanymi sterownikami – 2 szt.
- Monitory LCD lub LED 32’ ze zintegrowanymi sterownikami – 15 szt.
- Monitory LCD lub LED 46’ ze zintegrowanymi sterownikami – 13 szt.
- Totemy dedykowane pod monitory umożliwiające montaż monitorów 46’ – 12 szt.
- Stacje robocze FIDS wraz z konfiguracją i oprogramowaniem FIDS 2 szt.
- Mobilne stacje robocze FIDS wraz z konfiguracją i oprogramowaniem FIDS 2 szt.
- Serwery systemu FIDS wraz oprogramowaniem 2 szt.
- Interfejs do systemu FIS
- Interfejs do systemu generowania komunikatów głosowych GKS
- Interfejs do przesyłu danych na stronę internetową Portu

Zakres wykonawczy systemu

Zakres realizacji systemu:

- Dostawa,
- Wdrożenie systemu wizualnej informacji dla pasażerów FIDS (Flight Information Display System) będącego odrębnym systemem informatycznym pobierającym informację z systemu FIS (Fly Information System) poprzez dedykowany interfejs,
- zapewnienie integracji systemu FIDS z:
    - systemem FIS
    - z systemem generowania komunikatów głosowych SGKG,
    - serwisem internetowym
- Przygotowanie personelu lotniska do samodzielnej obsługi i administrowania systemem,
- przeszkolenie personelu lotniska w zakresie obsługi systemu FIDS,
- przeszkolenie administratorów w zakresie wymaganym przez dostawcę do bieżącej konserwacji systemu,
- opracowanie i wdrożenie procedur awaryjnych na wypadek awarii łączy systemu,
- umożliwienie rozbudowy systemu o nowe monitory systemu FIDS np. w przypadku modernizacji lotniska bez konieczności zmian programistycznych w systemie,
- przeprowadzenie wszystkich niezbędnych uzgodnień w zakresie koniecznym do uruchomienia systemu,
- dokumentację techniczną, instrukcje obsługi i utrzymania w języku polskim i angielskim.

Wymagania instalacyjne

System działa w oparciu o instalacje:

- sieć wewnętrzna LAN 1 Gbit na terenie Portu (w sieci muszą być włączone wszystkie elementy systemu)
- zasilanie dla serwerów, stacji roboczych, urządzeń wyświetlających opcjonalnie z zasilania bezprzerwowego lub przez urządzenia zasilanie awaryjne UPS
- dostęp do systemu FIDS przez Internet według zasad bezpieczeństwa obowiązujących w Porcie

Wymagania i specyfikacje sprzętowe

Monitory LED

Specyfikacja przykładowa:

- Light Source Type LED
- Type 60Hz LED BLU
- Resolution 1920x1080 (16:9)
- Pixel Pitch(mm) 0.17675(H) X 0.53025(V)
- Active Display Area 1018.08(H) X 572.67(V)
- Brightness 700nit
- Contrast Ratio (Dynamic) 4000:1
- Viewing Angle (Horizontal/Vertical) 178:178
- Response Time (G-to-G) 8ms
- Display Color 16.7M
- Colour Gamut 70%
- Input RGB D-Sub, DVI-D, Display Port
- Video Component(VCBS common), HDMI
- Audio Stereo mini Jack
- Output RGB DP(Loop-out)
- External Control RS-232C(In/Out) thru Stereo Jack, RJ-45
- External Sensor IR, Ambient Light
- Montaż VESA

Sterowniki zintegrowane

Specyfikacja minimalna:

- Processor Cortex-A9 1GHz Dual Core CPU
- On-Chip Cache Memory L1 (I/D) : 32KB / 32KB L2 (Unified) : 512KB
- Clock Speed 1GHz Dual
- Main Memory Interface 8Gbyte DDR3 Dual 32bit DDR3-667 (1333MHz)
- Graphics 2D & 3D Graphics Engine - Up to 1920x1080. 32bpp - Supports OpenGL ES
- Storage (FDM) 8GB (2.0GB Occupied by O/S, 6GB Available)
- Multimedia Video Decoder - MPEG-1/2, H.264/AVC (Dual) - VC-1, JPEG, PNG Audio DSP (Decoder) - AC3 (DD), MPEG, DTS and etc.
- IO Ports USB 2.0 * 2EA
- Operating System Linux

Totemy/obudowy dedykowane pod monitory umożliwiające montaż monitorów 46’

Wymagania minimalne dla totemów:

- totemy jednostronne
- budowa modułowa
- obudowa umożliwiająca łatwy dostęp do monitora
- obudowa zapewniająca odpowiednia warunki pracy – temperaturę i wentylację monitora
- szyba hartowana
- kotwienie do posadzki lub montaż bokiem do ściany
- praca wewnątrz budynku
- kolor czarny
- logotypy Portu podświetlane diodami LED
- nadruk na obudowie

Stacje robocze FIDS wraz z konfiguracją i oprogramowaniem FIDS

Wymagania minimalne stacji roboczych:

- monitor min. 22"
- jednostka PC o minimalnych parametrach:
- procesor min. 3,14 GHz
- pamięć RAM min. 3,5 GB
- dysk HDD 250 GB lub większy
- karta sieciowa 10/100/1000 Mbit/s
- system operacyjny Windows 7 Ultimate lub wyższy
- gniazda odpowiednie do stosowanych urządzeń peryferyjnych
- klawiatura i mysz

Mobilne stacje robocze FIDS wraz z konfiguracją i oprogramowaniem FIDS

Wymagania minimalne mobilnych stacji roboczych:

- Klasa procesora: i3-2330M;
- Prędkość procesora: 2,2 GHz;
- Częstotliwość szyny QPI/DMI: 5 GT/s;
- Pojemność pamięci podręcznej: 3 MB;
- Technologia Hyperthreading: Tak;
- Pojemność dysku (HDD): 320 GB;

- Rodzaj dysku: Standardowy (nośnik magnetyczny);
- Zainstalowana pamięć: 2048 MB;
- Przekątna ekranu LCD: 15,6 cali; Typ ekranu: TFT HD [LED];
- Maksymalna rozdzielczość LCD: 1920 x 1080;
- Złącza zewn.: 1x 15-stykowe D-Sub (wyjście na monitor),
- 1 x HDMI, 1x USB 2.0,
- 2x USB 3.0, 1x RJ-45 (LAN),
- 1x USB 2.0/eSATA,
- Bezprzewodowa karta sieciowa: Tak;
- Bluetooth: Tak;
- Zainstalowany moduł WWAN/3G:
- Czytnik kart pamięci: Tak;
- Typy odczytywanych kart pamięci: SecureDigital Card, SecureDigital Card High-Capacity (SDHC), SecureDigital eXtended Capacity Card (SDXC), MultiMedia Card, MemoryStick, MemoryStick Pro, xD-Picture Card;
- Karta sieciowa: 1x10/100/1000BaseT Gigabitethernet (RJ45),
- Głośniki stereo,
- Mikrofon,
- Zintegrowana kamera,
- Czytnik linii papilarnych;
- Zainstalowany system: Microsoft OEM Windows 7 Ultimate SP1 64 bit, Polish, 1pk, DVD,

Serwery systemu FIDS wraz oprogramowaniem

System będzie zainstalowany na dwóch identycznych serwerach rack 19” o następujących parametrach minimalnych:

- Procesor min: INTEL XEON X3450 PROCESSOR (2.66GHZ, 4C)
- Pamięć ram: 8GB (2X4GB DUAL RANK LV UDIMMS)
- Dyski twarde:2x 146GB SAS 6GBPS 10K 2.5" HYBRID HD pracujące w układzie RAID1.
- Napęd DVD:16X DVD+/-RW DRIVE SATA.
- Zasilacze: 2x REDUNDANT POWER SUPPLY (2 PSU) 400W .
- Zintegrowany kontroler zdalnego dostępu
- System operacyjny: SUSE LINUX ENTERPRISE SERVER 11 SP1

Zestawienie materiałów i licencji

SYSTEM FIDS

oprogramowanie FIDS	1
serwery systemowe z licencjami połączeń	2
licencja dla stacji graficznych	42
licencja dla stacji roboczych	2
interfejs do FIS	1
interfejs do systemu obsługującego komunikaty głosowe	1
interfejs do strony internetowej	1

SYSTEMEM GENEROWANIA KOMUNIKATÓW GŁOSOWYCH SGKG

systemem generowania komunikatów głosowych SGKG	1
interfejs do FIS	1
interfejs do DSO	1

SPRZĘT DO SYSTEMU FIDS

monitor 22"	2
monitor 32"	15
monitor 46"	13
totem 46"	12
uchwyt wraz z montażem	30
sterownik wewnętrzny	42
mobilne stacje robocze	1
stacja robocza z systemem operayjnym	1
serwer rakowy 19"	2

Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.

System informatyczny DCS

Oprogramowanie DCS jest specjalistycznym oprogramowaniem obsługującym odprawy przewoźników lotniczych. Proponowana platforma zapewnia łatwą konfigurowalność w zakresie systemowej odprawy pasażerskiej, z zachowaniem pełnego elektronicznego wsparcia procedur handlingowych, rozpoczynając od etapu planowania odprawy pasażerskiej a kończąc na obsłudze płytowej przewoźnika.

Zastosowanie pełnej integralności systemu pozwala na szybką implementację oprogramowania.

System DCS (Departure Control System) jest wyposażony w funkcje:

- odprawa pasażerska
- odprawa bagażowa
- obsługa statków powietrznych (planowanie załadunku i wyważanie)
- BRS – łączenie bagażu z pasażerem
- Funkcjonalność pod względem konfiguralności linki do systemów rezerwacyjnych najbardziej popularne Amadeus old BA, Amadeus Altea,KLM (codeco), Lufthansa System, Sabre ,SITA
- Obsługa API
- Obsługa pasażerów podróżujących w tranzycie
- Możliwość integracji na platformie typu CUTE
- Możliwość instalacji i integracji z kioskami (platforma CUSS)
- Obsługa rejsów kontenerowych
- Wsparcie dla załadunku Cargo
- Podlotowa kontrola rejsu
- Automatyczne wysyłanie depesz.

Wymagania sprzętowe

Serwer systemu DCS

Obudowa typu Rack , wysokość nie więcej niż 2U, dostarczona wraz z szynami i prowadnicą kabli.

Procesor sześciordzeniowy w architekturze x86, osiągające w testach wydajnościowych SPECint_rate2006 min. 163 pkt.

Płyta główna:

- minimum 18 gniazd pamięci RAM,
- karty rozszerzeń

- min 2 sloty PCI-Express Gen2 x8 typu low profile, możliwość obsadzania w min 2 slotach kart PCIe x16,
- min 5 slotów PCI-Express Gen2 x4, dwa z czterech gniazd PCI-Express Gen2 x4 mogą być wykorzystywane jako gniazdo x8, jeśli sąsiednie gniazdo będzie niewykorzystane
- min 10 portów USB (w tym min 3 z przodu, min 4 z tyłu, min 2 w środku),
- port VGA z tyłu,
- 2 porty RS-232 w tym jeden dostępny zarówno dla systemu operacyjnego jak i kontrolera zdalnego zarządzania
- możliwość użycia modułu szyfrowania TPM

Pamięć RAM nie mniej niż 8GB RAM typu registred DDR3-1333 z korekcją błędów Advanced ECC, funkcje scrubbing i SDDC, opcja aktywnej rezerwy i zapisu lustrzanego pamięci, obsadzone max 2 gniazda pamięci w trybie niezależnym, możliwość rozbudowy do minimum 192 GB.
HDD 4 szt dysków twardych typu SATA lub SAS hot-plug, nie mniejsze niż 300GB 15krpm 3,5” każdy, możliwość jednoczesnej instalacji dysków SATA i SAS, możliwość instalacji min. 6 szt. dysków,
Kontroler dysków typu SAS 6G minimum 8 portów z obsługą RAID 0,1,10,5,50,6,60 z pamięcią cache 512MB i podtrzymaniem bateryjnym, 2 kanałowy kontroler typu SATA
Napęd DVD- RW wewnętrzny,
panel serwisowy z wyświetlaczem LCD
Karta graficzna zintegrowana w jednym module z kontrolerem zdalnego zarządzania i pamięcią 32MB na płycie głównej, rozdzielczość min. 1600 x 1200
Karty sieciowe 2 typu Ethernet 10/100/1000 (akceleracja TCP/IP), rozruch PXE przez sieć LAN z serwera PXE, rozruch iSCSI przez zintegrowaną kartę sieci LAN, 1 karta Ethernet 10/100 wyłącznie dla komunikacji z kontrolerem zdalnego zarządzania
Zasilanie i chłodzenie Dwa redundantne zasilacze o mocy maksymalnej 800W na 1 zasilacz, zgodne ze standardem EPA, typu hot plug, o sprawności minimalnej 92% przy typowym obciążeniu 50%.
Nadmiarowe chłodzenie – redundantne wentylatory typu hot-plug.
Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (temperatura, dyski, zasilacze itd.).

Zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów.
Dedykowana karta LAN 10/100 Mb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera.
Wsparcie dla systemów operacyjnych Windows 2008, SUSE LINUX SLES-10 X86, Red Hat LINUX RHEL5 X86
Certyfikat producenta ISO 9001 w zakresie projektowania, produkcji i serwisu produktów, CE.

Komputer systemu DCS

Zaprojektowano komputer o minimalnych parametrach:
Procesor dedykowany do pracy w komputerach stacjonarnych, w architekturze x64 o wydajności min 4020 pkt w teście PassMark
Pamięć RAM 4GB DDR3-1333MHz w trybie dual channel
Dysk twardy 500GB (min. 7200 rpm, NCQ/6Gbit, 16MB cache)
Napęd Optyczny DVD+-RW wraz z licencjonowanym oprogramowaniem do nagrywania płyt CD/DVD
Płyta główna

- obsługa procesorów wielordzeniowych wspierających wirtualizację
- zintegrowany kontroler 3 x SATA
- min 1x PCI-Express 2.0 x16
- możliwość wyłączenia portów COM, LPT, USB, FDD z BIOS komputera bez pośrednictwa systemu operacyjnego, ani bez pośrednictwa urządzeń zewnętrznych
- możliwość ograniczenia dostępu do portów USB dla dysków, pamięci flash oraz HUBów pracujących w standardzie USB 1.x i 2.x;
- możliwość przekierowania konsoli tekstowej oraz ekranu konfiguracyjnego BIOS na stację zarządzającą przez sieć LAN
- wbudowany firewall sprzętowy działający niezależnie od obecności systemu operacyjnego, zarządzany i konfigurowalny zdalnie, nie widoczny dla systemu operacyjnego czy aplikacji,
- rozwiązanie sprzętowe zintegrowane w płycie głównej komputera zapewniające możliwość przywrócenia BIOS w przypadku jego uszkodzenia (ataki wirusów itp.) lub nieudanej aktualizacji bez pośrednictwa jakichkolwiek urządzeń zewnętrznych i w sytuacji, gdy obraz

na monitorze nie jest wyświetlany i/lub nie ma możliwości wprowadzania znaków za pomocą konsoli tekstowej czy uruchomienia systemu operacyjnego

- zintegrowany z płytą główną układ szyfrujący umożliwiający zaszyfrowanie poufnych dokumentów oraz poczty elektronicznej. Umożliwiający tworzenie zaszyfrowanych wirtualnych partycji. Usunięcie zabezpieczenia powoduje trwałe uszkodzenie płyty głównej a odczytanie zaszyfrowanych danych nie jest możliwe na innym urządzeniu. Układ zgodny ze standardem TPM 1.2
- Karta dźwiękowa zintegrowana, w standardzie High Definition, możliwość wyłączenia karty muzycznej w BIOS
- Karta sieciowa 10/100/1000 MBit/s
    - -obsługa protokołów: WoL, ASF 2.0, PXE 2.1
    - -możliwość wyłączenia karty sieciowej w BIOS
    - -możliwość odczytania adresu MAC karty z BIOS komputera
- Karta graficzna z możliwością dynamicznego przydzielania pamięci w obrębie pamięci systemowej, ze wsparciem dla DirectX 10.1, HDCP i OpenGL 2.1, np. Intel HD Graphics lub równoważna, możliwość pracy na dwóch ekranach jednocześnie, 1x DisplayPort
- Porty I/O
    - -min. 12 portów USB 2.0 zintegrowanych trwale w komputerze (w tym min. 4 na panelu przednim)
    - -min. 2x porty szeregowe
    - -2x porty PS2
    - -1x wyjście słuchawkowe oraz 1x wejście mikrofonowe na panelu przednim obudowy
    - -1x DVI, 1x port równoległy
    - -nie dopuszcza się możliwości zasłonięcia złączy USB znajdujących się na panelu przednim jakimikolwiek zaślepkami, maskownicami utrudniającymi wzrokową weryfikację ich użycia – np. obecności klucza USB czy innego urządzenia podłączonego do złączy na panelu przednim obudowy komputera
    - System operacyjny Windows 7 Professional 64bit z prawami do instalacji Windows XP Professional w polskiej wersji językowej. Preinstalowany fabrycznie na dysku twardym.
- Obudowa
        - -małogabarytowa
        - -fabrycznie przystosowana do pracy w pionie i w poziomie
        - -w kolorze ciemnym (szara, czarna)

- -zasilacz z aktywnym filtrem PFC o sprawności minimum 87% przy pełnym obciążeniu komputera
- -licencja na system operacyjny oraz numer seryjny komputera umieszczony na górnej części obudowy
- -slot Kensington umieszczony z tyłu obudowy
- -obudowa musi posiadać czujnik otwarcia obudowy wraz z logowaniem otwarcia, współpracujący z dostarczoną aplikacją zarządzając
- -obudowa musi posiadać zintegrowany zamek obudowy (nie dopuszcza się kłódek lub zabezpieczeń wystających poza obrys obudowy z jakiejkolwiek strony)

- Klawiatura PS2 w układzie polski programisty
- Mysz optyczna 800 dpi, PS2/USB, dwuprzyciskowa, rolka (scroll) jako trzeci przycisk, funkcja scroll'a czterokierunkowego.

Zarządzanie zdalne i diagnostyka. Oprogramowanie wyprodukowane i wspierane przez producenta komputera wraz z licencją do zarządzania w sieci, pozwalające minimum na:

- pracę w architekturze serwer-klient - licencja musi pozwalać na pełne wykorzystanie aplikacji w wymaganym zakresie
- możliwość zdalnego przypisania dla jednego, lub grupy komputereów unikalnego numeru inwentarzowego widocznego zdalnie dla administratora jak i bezpośrednio w BIOS maszyny
- monitoring systemu i przekazywanie informacji o zdarzeniach na stację administratorską (konsola graficzna na stacji zarządzającej, konsola tekstowa, email, sms)
- możliwość konfiguracji i weryfikacji zakresu i stopnia szczegółowości alertów przekazywanych na stację administratorską oraz wybór sposobu informacji o zdarzeniu
- monitoring komponentów takich jak: dysu twardy (SMART), pamięci, wentylatorów, stanu czujnika otwarcia obudowy, monitoring temperatury wewnętrznej komputera
- zdalne zarządzanie BIOS: wprowadzanie i zmiana haseł BIOS, archiwizacja i aktualizacja BIOSu dla pojedynczego komputera i grupy komputerów jednocześnie; modyfikacja sekwencji bootowania;
- generowanie raportów dot. pojedynczych komputerów lub grup komputerów, w zakresie zainstalowanych komponentów, systemu operacyjnego oraz aplikacji
- inwentaryzacja szczegółowa komputera:
    - -odczyt modelu, numeru seryjnego i numer inwentarzowego komputera
    - wersja i model płyty głównej, wersja BIOS;

- model, wersja firmware i numer seryjny dysku twardego,
- model, wersja firmware i numer seryjny napędu optycznego
- i sposób obsadzenia kości pamięci wraz z informacją o zainstalowanych kościach (pojemność, oznaczenie, numer seryjny kości)

- Deklaracja zgodności CE,
- Certyfikaty jakości ISO 9001 i 14001,
- Certyfikat ISO9001 dla serwisu,
- Zgodność z normami EN55022/B, EN55024, EN61000-3-2/3,
- Certyfikacja Energy Star w wersji co najmniej 5.0 dla oferowanego modelu komputera,
- Poziom emitowanego hałasu, mierzony wg normy ISO 7779 i wykazany według normy ISO 9296 w trybie jałowym (tryb IDLE przy uruchomionym systemie Microsoft Windows 7 lub Vista Business) powinien wynosić nie więcej niż 22 dB.

Kiosk do samodzielnej odprawy pasażerów

Wyposażenie kiosku:

2) Czytnik Paszportu
3) czytnik kart kredytowych
4) drukarka kart pokładowych
5) drukarka zawieszek bagażowych
6) mechanizm umożliwiający łatwą i prosta wymianę papieru
7) mechanizm aktywacji kiosku w tryb konserwacji
8) otwieranie ekranu dotykowego do góry w trybie normalnej pracy
9) oprogramowanie pozwalające na zdalne monitorowanie
10) zgodność ze standardem IATA CUSS
11) wyposażony w rozwiązania ułatwiające szybki transport kiosku w obrębie terminala.

Parametry techniczne

Ekran dotykowy

- 17 calowy TFT, szerokokątny, kolorowy wyświetlacz LCD
- Rozdzielczość: 1280 x 1024 pikseli, 300 cd

Wyposażenie w komputer PC o wymaganiach minimalnych:

- Industrial PC z 80 GB twardym dysku Pentium M lub Core 2 Duo, do 4 GB pamięci RAM
- WIN XP Pro
- Dual 10/100 Base Tx Fast Ethernet

- 2 x RS232 z możliwością przedłużenia
- 4 x USB Hub z możliwością przedłużenia
- Karta WiFi

Wyposażenie w czytniki kart o wymaganiach minimalnych:
- Manual DIP Hybrid ISO 3
- Opcjonalnie czytnik kart bezstykowych RF

Wyposażenie w drukarkę kart pokładowych o wymaganiach minimalnych:
- Technologia: 300 dpi termiczna 1D/2D z kodami kreskowymi (Tj. Code 39, 128, PDF 417)

Drukowanie parametry:
- Szerokość: 200 mm (7,87 in)
- Długość: 82,5 mm (3.24 in)
- Grubość papieru: 80 - 120 g
- Automatyczne odcinanie
- Prędkość druku: 50 mm / s (2 w / s)
- Papier: 2500 ATB rozmiar, rozmiar A4

Wyposażenie w czytniki kodów kreskowych o wymaganiach minimalnych:
- Matryca CCD do czytania kodów kreskowych 1D/2D
- Wielokierunkowy przebieg
- Interpretacja kodów 2D : PDF 417, Datamatrix, Aztec i QR Code
- Interpretacja kodów kreskowych 1D, Code 128, Code 39, Interleaved 2 z 5, UPC / EAN, Codabar

Wyposażenie w skaner paszportu:
- Przesuwny czytnik OCR (moduł przeciw-top)

Wyposażenie w drukarkę zawieszek bagażowych:
- zgodna z IATA standard Cuss 21

Zgodności
- CE, FCC część 15, UL / CSA (w trakcie)
- Standard ADA dla dostępu pasażerów podróżujących na wózkach inwalidzkich

- IATA / ATA CUSS

Certyfikaty

f) Potwierdzenie kompatybilności producenta systemu DCS na daną platformę systemową

g) Potwierdzenie odczytu kodów 2D zgodnych z dyrektywami IATA.

W zakresie dostawy jest również dostawa 100000 standardowych kart boardingowych oraz 100000 standardowych przywieszek bagażowych.

Zestawienie urządzeń i licencji

Lp	Typ	Nazwa	Ilość
1	Oprgramowanie DCS	zgodnie z opisem	1
2	Serwer	zgodnie z opisem	1
3	Komputer	zgodnie z opisem	12
4	Kiosk dla pasażera	zgodnie z opisem	2
5	oprogramowanie kiosku	zgodnie z opisem	1
6	wyposażenie check in	Drukarka Boardingowe	7
7	wyposażenie check in	Drukarka zawieszek	7
8	wyposażenie check in	Klawiatury z czytnikiem dokumentow	7
9	Drukarka DPD	zgodnie z opisem	3
10	wyposażenie gate	Gatereader	3
11	wyposażenie bagażowni	zgodnie z opisem	1
12	Router	zgodnie z opisem	1
13	Switch	zgodnie z opisem	1
14	oprogramowania antywirusowe	Oprogramowanie zgodnie z opisem lub równoważne	13

Przytoczone zostały nazwy elementów systemu odnoszących się do konkretnych produktów dostępnych na rynku. W świetle art. 29 ust. 3 ustawy PZP należy je traktować jako urządzenia przykładowe – powołanie się na konkretny produkt nie oznacza konieczności jego zastosowania. Dopuszcza się stosowanie urządzeń zamiennych cechujących się parametrami nie gorszymi niż cechujące urządzenia podane poniżej. Wprowadzone zmiany nie powinny w żaden sposób uszczuplać funkcjonalności systemu.