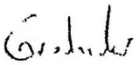
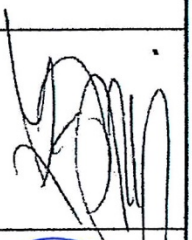
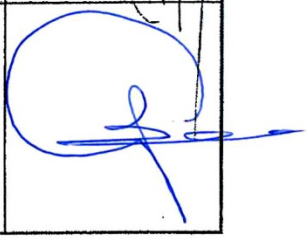
„MICROSYSTEM” Sp. z o.o.
81-730 SOPOT ul. Bitwy pod Płowcami 38/6-9 NIP: 585-000-19-80
adres do korespondencji:
80-299 GDAŃSK, ul. Nowy Świat 34 tel. 58 551 09 72 fax. 58 551 78 42 e-mail: biuro@microsystem.com.pl www.microsystem.com.p

Projekt koncepcyjny integracji elektronicznych systemów zabezpieczeń budynków i terenów Zarządu Morskiego Portu Gdynia S.A.

Branża	Imię i nazwisko	Uprawnienia	Data	Podpis
Systemy Bezpieczeństwa	Adrian Grodzicki	PISA SA1-SA4: 1148/P/2008	30.11.2017.	
	Zbigniew Świrkowicz	PISA SA1-SA4: 71/P/98, PISA 2466/KW/2011	30.11.2017.	
	Grzegorz Zięba	PISA SA1-SA4: 3245/P/2013	30.11.2017.	
Architektura	Arkadiusz Marszałkowski	6153/GD/94	30.11.2017.	
Elektryczna	Marcin Burzyński	4594/Gd/90	30.11.2017.	
Telekomunikacyjna	Artur Baranowski	2015/00/U	30.11.2017.	
Zatwierdził:	Georgis Bogdanis Ekspert PISA certyfikat 031	Koncesja MSWiA L-0428/00	30.11.2017.	

Sopot, listopad 2017

UZGODNIENIA BRANŻOWE

Branża	Imię i Nazwisko	Uprawnienia	Podpis
Architektoniczna	Arkadiusz Marszałkowski	Uprawnienia do wykonywania samodzielnej funkcji projektanta w specjalności architektonicznej nr 6153/GD/94	
Elektryczna	Marcin Burzyński	Uprawnienia do wykonywania samodzielnej funkcji projektanta w specjalności inżynieryjno instalacyjnej w zakresie sieci i instalacji elektrycznych nr 4594/Gd/90	
Telekomunikacyjna	Artur Baranowski	Uprawnienia Budowlane do projektowania i kierowania robotami budowlanymi w specjalnościach instalacyjnych w telekomunikacji przewodowej wraz z infrastrukturą towarzyszącą bez ograniczeń nr 2015/00/U	
Teletechniczna	Adrian Grodzicki	Kwalifikowany pracownik zabezp. technicznego nr PZT-19860 Pracownik zabezp. technicznego drugiego stopnia – projektowanie systemów zabezpieczeń technicznych klas SA1-SA4 Dyplom Polskiej Izby Systemów Alarmowych nr 1148/P/2008	
Teletechniczna	Grzegorz Zięba	Kwalifikowany pracownik zabezp. technicznego nr PZT-19857 Pracownik zabezp. technicznego drugiego stopnia – projektowanie systemów zabezpieczeń technicznych stopni 1-4. Dyplom Polskiej Izby Systemów Alarmowych nr 3245/P/2013	
Teletechniczna	Zbigniew Świrkowicz	Kwalifikowany pracownik zabezp. technicznego nr PZT-6977 Projektowanie systemów zabezpieczeń technicznych stopni 1-4 do klasy SA4 Dyplom Polskiej Izby Systemów Alarmowych nr 2466/KW/2011 oraz nr 71/P/98	
Teletechniczna	Georgis Bogdanis	Kwalifikowany pracownik zabezpieczenia technicznego nr PZT-4521; Certyfikat **eksperta** Polskiej Izby Systemów Alarmowych w zakresie bezpieczeństwa nr 031; Certyfikat Manager Systemu Zarządzania Bezpieczeństwem Informacji wg ISO 27001:2005	

UZGODNIENIA SŁUŻB PORTOWYCH

Stanowisko	Imię i Nazwisko	Zakres	Podpis
Kierownik Działu Ochrony Portu	Józef Lis	Dział Ochrony Portu	
Kierownik Działu Informatyki i Telekomunikacji	Stanisław Lachowski	Teleinformatyka	
Komendant PSP	Grzegorz Bulwa	Portowa Straż Pożarna	

Spis treści

Słownik pojęć

- **Centrala sygnalizacji pożarowej (SSP)-** centralna część instalacji sygnalizacji pożarowej, zasilająca czujki pożarowe oraz odbierająca od nich sygnały o wykryciu pożaru w celu wywołania alarmu i w razie potrzeby przekazujące je dalej do straży pożarnej lub do automatycznych urządzeń zabezpieczających, przeciwpożarowych, a także automatycznie kontrolująca sprawność całej instalacji.
- **Punkt alarmowy Portowej Straży Pożarnej (PSP) (SSP)-** - stacja ze stałym dozorem, w którym są odbierane zgłoszenia o niebezpieczeństwie i podejmowane są działania zmierzające do mobilizacji ludzi, urządzeń i wyposażenia.
- **Część składowa , element składowy (SSP) -** urządzenie stanowiące część systemu sygnalizacji pożarowej, objęte zakresem któregokolwiek arkusza normy.
- **Czujka-** urządzenie wykrywające zagrożenie.
- **System sygnalizacji pożarowej (SSP)-** zbiór kompatybilnych elementów, które, gdy tworzą instalację o określonej konfiguracji, są zdolne do wykrycia pożaru, inicjowania alarmu i innych stosowanych działań.
- **Alarm-** ostrzeżenie o istnieniu zagrożenia dla życia, mienia lub zdrowia.
- **System sygnalizacji włamania i napadu (SSWiN)-** System alarmowy do wykrywania i sygnalizowania, wejścia albo usiłowania wejścia intruza do miejsca chronionego, oraz sygnalizowania wyzwolenia urządzenia sygnalizacji napadu.
- **Elementy systemu (SSWiN)-** pojedyncze urządzenia, które tworzą SSWiN, gdy są wspólnie skonfigurowane.
- **Miejsce chronione (SSWiN)-** część budynku i / lub terenu , w którym włamanie, usiłowanie włamania, lub wyzwolenie urządzenia do sygnalizacji napadu może być wykryte przez SSWiN.
- **Nadajnik / odbiornik miejsca chronionego-** urządzenie w miejscu chronionym, zawierającego interfejs, do systemu alarmowego oraz interfejs do sieci transmisji alarmu.
- **Sabotaż-** umyślne zakłócenie działania SSWiN lub jego części.
- **Użytkownik-** osoba uprawniona do obsługi danego systemu.
- **System CCTV, system dozorowy CCTV-** system składający się z punktów kamerowych, urządzeń kontrolnych oraz urządzeń do przesyłu i sterowania, system może być niezbędny do dozorowania określonej strefy bezpieczeństwa.
- **Kamera CCTV-** urządzenie zawierające przetwornik obrazu, wytwarzający sygnał wizyjny z obrazu optycznego.

Słownik pojęć

- **Punkt kamerowy CCTV-** Zestaw zawierający kamerę CCTV oraz odpowiedni obiektyw i niezbędny osprzęt pomocniczy.
- **Monitor wizyjny-** urządzenie przetwarzające sygnał wizyjny na obrazy wyświetlane na ekranie.
- **Videowall (wallscreen) -** zespół dwóch lub więcej monitorów, służących do wyświetlania sygnałów wizyjnych.
- **Rejestrator-** część systemu CCTV służąca do rejestracji sygnału wizyjnego.
- **Dostęp-** funkcjonowanie wejścia do lub wyjścia z obszaru kontrolowanego.
- **System kontroli dostępu (KD)-** system obejmujący wszystkie składniki konstrukcyjne i organizacyjne oraz te, które odnoszą się do urządzeń, niezbędnych do sterowania dostępem.
- **Centralka kontroli dostępu-** Urządzenie, które podejmują decyzję o odblokowaniu jednego lub kilku przejść kontrolowanych i zarządza związaną z tym faktem sekwencją sterowania.
- **Czytnik przejścia kontrolowanego-** urządzenie służące do wydobycia danych rozpoznawanych z identyfikatora lub biometryki. Urządzenie może być wyposażone we współpracującą z nim klawiaturę, jeżeli jest stosowane z wykorzystywaniem informacji zapamiętanych.
- **Zdarzenie (KD)-** zmiana zachodząca w obrębie systemu KD.
- **Identyfikator-** dane rozpoznawcze zawarte na kartach, kluczach etykietach, przywieszkach, itp. nośnikach.
- **Integracja-** proces polegający na zespoleniu systemów tak, aby mogły one korzystać nawzajem ze swoich zasobów.
- **Integrator-** program komputerowy pozyskujący dane z przynajmniej dwóch systemów, który pozwala na korzystanie z ich zasobów.
- **Poziom integracji-** zakres integracji poszczególnego systemu.
- **Cykl życia technologicznego –** wszelkie możliwe, kolejne fazy istnienia danego produktu, w ujęciu technicznym.
- **Kres cyklu życia technologicznego –** przedostatni etap cyklu życia technicznego, charakteryzujący się wysokim stopniem wyeksploatowania, zwiększoną awaryjnością, ograniczoną zdolnością wykonywania zadań.
- **Serwer systemu integracyjnego-** urządzenie z zainstalowanym oprogramowaniem integratora.
- **Serwer redundantny systemu integracyjnego-** urządzenie z zainstalowanym oprogramowaniem integratora, które może przejąć obowiązki serwera systemu integracji.
- **Klient (system integracyjny)-** komputer z zainstalowanym oprogramowaniem, pozwalającym na użytkowanie, bądź administrowanie integratora

Streszczenie

Niniejszy dokument przedstawia projekt koncepcyjny integracji elektronicznych systemów zabezpieczeń budynków i terenów zarządzanych przez Zarząd Morskiego Portu Gdynia. Zalicza się do nich Systemy Sygnalizacji Włamania i Napadu, Telewizji Dozorowej CCTV, Systemy Kontroli Dostępu i Systemy Sygnalizacji Pożaru.

Opracowaniem objęto budynki biurowe, użytkowane przez ZMPG jak i wynajmowane podmiotom zewnętrznym, hale magazynowe, budynki peryferyjne (posterunki itp.) oraz poszczególne punkty kamerowe, znajdujące się na terenie portu.

W ramach opracowania zaproponowano wybudowanie w budynku PSP Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń. Przedstawiono koncepcję zagospodarowania pomieszczeń wraz z niezbędną infrastrukturą. Określono wymogi funkcjonalne i minimalne parametry techniczne systemu i sprzętu informatycznego.

Zaproponowano również przeniesienie Punktu alarmowego PSP, z pomieszczenia z budynku przy ul. Rotterdamskiej 9 do budynku PSP przy ul. Chrzanowskiego 15.

Program funkcjonalno – użytkowy zawiera również zaproponowany poziom integracji poszczególnych systemów zabezpieczeń.

Przedstawiono również koncepcję dostosowania do projektu, a w razie konieczności rozwoju, sieci teleinformatycznych wraz z niezbędną infrastrukturą. W określonych miejscach zaproponowano użycie zasilania gwarantowanego, zastosowania systemu klimatyzacji itp.

Dokument wskazuje również systemy, które powinny zostać zmodernizowane, ze względu na brak możliwości integracji oraz osiągnięcia lub zbliżenie się systemów do końca cyklu życia technologicznego.

W ramach koncepcji określono wymagania dla przyszłego Wykonawcy,

Dokument przedstawia również uproszczony kosztorys inwestorski.

Spis Rysunków

Podstawa opracowania

1. Umowa nr. 59/AP/I/2017 o wykonanie prac projektowych, zawarta w Gdyni 29.08.2017r.
2. Wizje lokalne we wskazanych obiektach, które wyposażone są w elektroniczne systemy zabezpieczeń.
3. Analiza dokumentacji powykonawczych.
4. Wywiady z pracownikami obsługującymi istniejące systemy.
5. Spotkania z branżystami.
6. Panele dyskusyjne z pracownikami ZMPG.
7. Analiza dostępnych rozwiązań rynkowych.
8. Doświadczenie Wykonawcy.
9. Przepisy prawne i normatywne:

PN-EN 62676-1-1:2014-06/AC:2014-09E - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 1-1: Wymagania systemowe -- Postanowienia ogólne

PN-EN 62676-1-1:2014-06E - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 1-1: Wymagania systemowe -- Postanowienia ogólne

PN-EN 62676-1-2:2014-06/AC:2015-07E - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 1-2: Wymagania systemowe -- Wymagania eksploatacyjne dotyczące transmisji wizji

PN-EN 62676-2-1:2014-06E - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 2-1: Protokoły transmisji wizji -- Wymagania ogólne

PN-EN 62676-2-2:2014-06E - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 2-2: Protokoły transmisji wizji – Zastosowanie międzyoperacyjności IP oparte na usługach HTTP i REST

PN-EN 62676-2-3:2014-06E - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 2-3: Protokoły transmisji wizji -- Zastosowanie międzyoperacyjności IP oparte na usługach Web

PN-EN 62676-4:2015-06E - Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 4: Wytyczne stosowania

PN-EN 50131-1:2009/A2:2017-07E - Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 1: Wymagania systemowe

PN-EN 60839-11-32:2017-07E - Alarmowe i elektroniczne systemy zabezpieczeń -- Część 11-32: Elektroniczne systemy kontroli dostępu -- Monitorowanie kontroli

Podstawa opracowania

dostępu oparte na usługach Web

PKN-CLC/TS 50131-7:2011P - Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 7: Wytyczne stosowania

PN-EN 60839-11-2:2015-08/AC:2015-12E - Systemy alarmowe i elektroniczne systemy zabezpieczeń -- Część 11-2: Elektroniczne systemy kontroli dostępu -- Wytyczne stosowania

PN-EN 60839-11-2:2015-08E - Systemy alarmowe i elektroniczne systemy zabezpieczeń -- Część 11-2: Elektroniczne systemy kontroli dostępu -- Wytyczne stosowania

PN-EN 50136-1:2012P - Systemy alarmowe -- Systemy i urządzenia transmisji alarmu -- Część 1: Wymagania ogólne dotyczące systemów transmisji alarmu

PN-EN 60839-11-31:2017-07E - Alarmowe i elektroniczne systemy zabezpieczeń -- Część 11-31: Elektroniczne systemy kontroli dostępu -- Podstawowy protokół międzyoperacyjności oparty na usługach Web

PN-EN 60839-11-1:2014-01E - Systemy alarmowe i elektroniczne systemy zabezpieczeń -- Część 11-1: Elektroniczne systemy kontroli dostępu -- Wymagania dotyczące systemów i części składowych

PN-EN 54-1:2011 - Systemy sygnalizacji pożarowej

PN-EN 50518-1:2014-07E - Centrum monitoringu i odbioru alarmu -- Część 1: Wymagania dotyczące rozmieszczenia i konstrukcji

PN-EN 50518-2:2014-07E - Centrum monitoringu i odbioru alarmu -- Część 2: Wymagania techniczne

PN-EN 50518-3:2014-07E - Centrum monitoringu i odbioru alarmu -- Część 3: Procedury i wymagania dotyczące działania

I. KONCEPCJA INTEGRACJI ELEKTORNICZYNYCH SYSTEMÓW ZABEZPIECZEŃ.

1. Inwentaryzacja systemów bezpieczeństwa

Obiekty ZMPG podzielone zostały na 3 kategorie:

- Obiekty w pełni wykorzystywane przez ZMPG.
- Obiekty częściowo, lub w całości wynajmowane, z systemami zabezpieczeń przeznaczonymi do integracji.
- Obiekty bez integrowanych systemów zabezpieczeń.

W pierwszej kategorii zawierają się obiekty i tereny, w których wszystkie systemy i ich składowe przeznaczone są do integracji.

Punkt drugi obejmuje obiekty i tereny, w których istnieją systemy zabezpieczeń elektronicznych, jednak nie wszystkie ich elementy przeznaczone są do integracji. Należy pominąć elementy systemów, podlegające administracji najemców obiektów, czyli poszczególne składowe KD, SSWiN i CCTV, SSP natomiast powinno być w pełni kontrolowane przez ZMPG.

Trzeci punkt to obiekty które nie mają systemów zabezpieczeń elektronicznych pozostających w całości lub w części w gestii ZMPG.

Stosując przedstawione wytyczne przeprowadzono wizje lokalne obiektów i terenów, przeprowadzono wywiady z pracownikami ZMPG, dokonano analizy dokumentacji powykonawczych.

W ramach tych prac zinwentaryzowano:

- Ilości central pożarowych, włamaniowych, kontrolerów KD i rejestratorów CCTV.
- Ilości elementów aktywnych w tych systemach:
- Dla SSP - liczbę central, czujek i modułów.
- Dla SSWiN - liczbę central i czujek
- Dla KD - liczbę kontrolerów i przejść.
- Dla CCTV - liczbę rejestratorów i kamer.
- Informacje o cyklu życia technologicznego poszczególnych podsystemów.
- Ilość i lokalizację węzłów teleinformatycznych.

Zebrane ilości należy traktować jako liczby szacunkowe i nie powinno się tworzyć projektu wykonawczego bez przeprowadzenia szczegółowej inwentaryzacji.

1.1. CCTV

System telewizji dozorowej CCTV łączy w sobie kilka funkcji z dziedziny bezpieczeństwa. Umożliwia obserwacje w czasie rzeczywistym, analizę zdarzeń poprzez przeglądanie nagrań, realizuje funkcję prewencyjną.

Żeby zrealizować cel integracji należy przyjąć, że najlepszą technologią jest rozwiązanie oparte o sieci IP. W zakresie podstawowym przewidziano sieciowanie na poziomie rejestratorów. W zakresie optymalnym, wszystkie podzespoły powinny działać w technologii IP.

Tabela poniżej przedstawia ilości elementów CCTV, które Zamawiający wskazał jako przeznaczone do integracji.

Tabela 1 Elementy CCTV przeznaczone do integracji

L.P	Producent / typ	Liczba rejestratorów	Liczba kamer
1	Axis	2	100-120
2	Hikvision	4	47
3	UTC	1	12
4	Pelco	2	25
5	Samsung	6	46

System firmy Axis (tzw. "norweski") jest obecnie rozbudowywany. Należy zatem przyjąć, że integracją objęte będą kamery w ilości ok. 100-120 sztuk. Swoim zasięgiem obejmuje cały teren Portu, zarówno wewnętrzny jak i zewnętrzny. Ze względu na jego wykorzystanie, między innymi przez Służbę Celną, zdecydowano na częściową integrację. Polegać ma ona na przechwytywaniu tylko strumieni video, bez możliwości zarządzania urządzeniami czy pobierania materiału video.

System firmy Hikvision jest obecnie rozbudowywany. Docelowo urządzenia tego producenta zastąpią urządzenia innych firm, oprócz systemu monitoringu opartego o rozwiązania Axis'a. W zależności od obiektu, do integracji przeznaczone będą wszystkie zainstalowane urządzenia lub tylko wybrane, pozostające w gestii ZMPG.

Systemy UTC, Samsunga i Pelco nie są przeznaczone do rozbudowy. ZMPG przewiduje zastąpienie ich, w przypadku osiągnięcia przez nie końca cyklu życia technologicznego, innymi rozwiązaniami. W miarę możliwości integratora oraz w zależności od obiektu, do integracji przeznaczone będą wszystkie zainstalowane urządzenia lub tylko wybrane, pozostające w gestii ZMPG.

1.2. SSWiN

System Sygnalizacji Włamania i Napadu stosowany jest do wykrycia zagrożenia w objętych nim pomieszczeniach i obiektach.

Żeby zrealizować cel integracji należy przyjąć, że najlepszą technologią jest rozwiązanie oparte o sieci IP.

Tabela poniżej przedstawia ilości elementów SSWiN, które Zamawiający wskazał jako przeznaczone do integracji.

Tabela 2 Elementy SSWiN przeznaczone do integracji

L.P.	Producent / typ	Liczba central	Liczba czujek
1	ATS Master	1	134
2	Satel	30	612
3	Roconet	5	34

Zamawiający przyjął rozwiązania firmy Satel jako wiodące w zakresie SSWiN. Docelowo powinny one zająć miejsce innych systemów alarmowych. Systemy te zostaną objęte integracją.

ATS Master w funkcji SSWiN przewidziany jest do integracji.

System Roconet obejmuje kilka pomieszczeń w budynku Zarządu. Przeznaczony jest do wymiany na rozwiązania Satela.

1.3. KD

Poprzez system Kontroli Dostępu należy rozumieć takie rozwiązanie, które umożliwia zarządzanie ruchem osób i pojazdów w oparciu o identyfikatory elektroniczne, kontrolery i urządzenia aktywne.

Żeby zrealizować cel integracji należy przyjąć, że najlepszą technologią jest rozwiązanie oparte o sieci IP.

Tabela poniżej przedstawia ilości elementów KD, które Zamawiający wskazał jako przeznaczone do integracji.

Tabela 3 Elementy KD przeznaczone do integracji

L.P.	Producent / typ	Liczba kontrolerów	Liczba przejść
1	Unicard	53	54
2	ATS Master	6	6
3	Satel	1	1
4	Vemco	10	12

System firmy Unicard jest obecnie rozbudowywany i należy go traktować jako wiodący system KD w Porcie. System przewidziany jest do integracji.

System ATS Master jest przewidziany jest do integracji. Planowane jest jego zastąpienie przez urządzenia Unicard.

System Satel jest przewidziany jest do integracji.

System Vemco jest systemem wyniesionym i odpowiada za kontrolę przejść na posterunkach strażniczych. Wszystkie posterunki powinny zostać objęte integracją.

1.4. SSP

System Sygnalizacji Pożaru w Porcie stosowany jest do wykrycia zagrożenia pożarowego w objętych nim obiektach.

Żeby zrealizować cel integracji należy przyjąć, że najlepszą technologią komunikacji informacji a stanach czujek jest rozwiązanie oparte o sieci IP.

Tabela poniżej przedstawia ilości elementów CCTV, które Zamawiający wskazał jako przeznaczone do integracji.

Tabela 4 Elementy SSP przeznaczone do integracji

L.P.	Producent / typ	Liczba central	Liczba czujek
1	Schrack Seconet	5	813
2	Esser	3	747
3	Bosch	1	120
4	Autronica	1	253

System Autronica jest zainstalowany w Bazie Promowej, która przeznaczona jest do likwidacji. Pozostałe Systemy Sygnalizacji Pożaru przewidziane są do integracji.

1.5. Ujęcie zbiorcze systemów bezpieczeństwa

Poniższa tabela przedstawia ujęcie zbiorcze systemów i ich składowych przeznaczonych do integracji. Układ odzwierciedla rozmieszczenie urządzeń z podziałem na obiekty, w których zainstalowano rejestratory, kontrolery i centrale.

Zamawiający przyjął jako docelowe następujące standardy sprzętowe:

- dla SSWiN - Satel,
- dla KD - Unicard
- dla CCTV – Axis, Hikvision,
- dla SSP - Esser

Tabela 5 Szczegółowa inwentaryzacja elektronicznych systemów bezpieczeństwa

L.P	CCTV			KD			SSWiN			SSP		
	Rejestratory		Liczba kamer	Kontroler		Liczba przejść czytn.	Centrale		Liczba urządzeń	Centrala		Liczba czujek
	Producent	Ilość		producent	Ilość		Producent	Ilość		Producent	Ilość	
Rotterdamska 9	UTC Hikvision	1 1	21	Unicard	12	12	UTC Satel Roconet	1 1 3	29	Schrack	1	
Indyjska 13	Kamery działu IT		2	Unicard	3	5	Satel		256			brak
Magazyn K	Hikvision	1	18	Unicard Do rozbudowy GPD	20	20	Satel 2x centrale 6x ekspander	2	70	Esser	1	150
Magazyn H	Bez rej lokalnego		3	Unicard Roger (bez int)		5	satel	1	20	brak I		brak
Polska 13A Bud. Biurowo szkolny	Samsung	3	31	ATS Master Docelowo Unicard	6	6	Satel	5	100	Esser	1	210
Chrzanowskiego 15, 17 PSP	Samsung	1	4	Unicard	1	1	brak		brak	brak		brak
Polska 13	brak		brak	Brak		brak	Satel		20	brak		brak

Inwentaryzacja systemów bezpieczeństwa

L.P	CCTV			KD			SSWiN			SSP		
	Rejestratory		Liczba kamer	Kontroler		Liczba przejść czytn.	Centrale		Liczba urząd zeń	Centrala		Liczba czujek
	Producent	Ilość		producent	Ilość		Producent	Ilość		Producent	Ilość	
A1-A4 Kwiatkowskiego 60	Samsung		5	brak		brak	brak		brak	Schrack	1	532
Wiśniewskiego 31	Hikvision	1	10	Brak 6 pomieszczeń do unicardu		brak		3	134	brak		brak
Magazyn 12	Pelco	2	25	Satel Wspólna centrala z SSWiN		1	Satel Wspólna centrala z KD	5	100	Esser	1	387
Magazyn nr 6	Hikvision	1	10	Docelowo Unicard		1	Satel	2	50	Bosch	1	120
A1-IT Kwiatkowskiego 60	Axis	1	100	Unicard	8	8	Satel	1	35	brak		brak
Warsztatowa 4	brak		brak	Unicard	1	1	Satel	1	1	brak		brak
Polska 43	brak		brak	Unicard	1	1	Satel	1	3	brak		brak
Solidarności 1c	brak		brak	brak		brak	brak		brak	Schrack	1	110
Indyjska 1	brak		brak	brak		brak	brak		brak	Schrack	1	56
Baza promowa	brak		brak	brak		brak	satel	2	113	Autronica	1	252
Graniczny Punkt Kontroli Weterynaryjnej	brak		brak	Satel	2	12	Satel	2	12	Shrack	1	116
Rotterdamska 13	brak		brak	brak		brak	Satel	1	8	brak		brak

Inwentaryzacja systemów bezpieczeństwa

L.P	CCTV			KD			SSWiN			SSP		
	Rejestratory		Liczba kamer	Kontroler		Liczba przejść czytn.	Centrale		Liczba urząd zeń	Centrala		Liczba czujek
	Producent	Ilość		producent	Ilość		Producent	Ilość		Producent	Ilość	
Celna 5	brak		brak	brak		brak	Satel	1	12	brak		brak
Wiśniewskiego 23 Stacja pomp	brak		brak	brak		brak	Satel	1	12	brak		brak
Demela Zbiorniki	brak		brak	brak		brak	Satel	1	7	brak		brak
Węglowa 8 PZ	brak		brak	brak		brak	Roconet	1	10	brak		brak
Rotterdamska 7 PZ	brak		brak	brak		brak	Roconet	1	8	brak		brak
Czechosłowacka Budynek P-16	brak		brak	brak		brak	Satel	1	12	brak		brak
Budynek Magazynowy Chrzanowskiego 17	brak		brak	brak		brak	Satel	1	10	brak		brak

2. Punkty obsługi zdarzeń alarmowych.

Informacje o zdarzeniach alarmowych agregowane są dwa strumienie danych:

1. Dane z SSP
2. Dane z SSWiN

Każdy zbiór danych obsługiwany jest w wyspecjalizowanym stanowisku przez wykfalifikowanych pracowników.

Punkt alarmowy Portowej Straży Pożarnej mieści się w pomieszczeniu Dyspozytora Portu w budynku Zarządu Portu przy ul. Rotterdamskiej 9.

Pracownik ZMPG, z tego miejsca kieruje ruchem statków w porcie. Obsada stanowiska jest całodobowa. W celu sprawnego zarządzania wykorzystywana jest specjalne oprogramowanie oraz tablica sytuacyjna.

Punkt alarmowy Portowej Straży Pożarnej wykorzystuje specjalnie zaprojektowany i wykonany Pulpit Strażaka, który agreguje wszystkie sygnały SSP. Z tego miejsca podejmuje się wszelkie decyzje związane z obsługą zdarzeń alarmowych SSP. Stanowisko obsługiwane jest całodobowa przez wykfalifikowanego strażaka.

Zdublowany, nie wykorzystywany obecnie Punkt alarmowy PSP znajduje się w budynku PSP.

Centrum monitoringu alarmów SSWiN mieści się w budynku przy al. Solidarności 1A. Obecnie zajmuje jedno pomieszczenie. Obsługiwane jest całodobowo, przez pracowników firm ochroniarskich, wyposażonych w broń palną. Za pomocą dedykowanego komputera, monitorowane są alarmy i zdarzenia SSWiN. Obsługa korzysta również, z podglądu CCTV telewizji systemu Axis.

3. Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

Centrum będzie zlokalizowane w wyremontowanych pomieszczeniach na 2 piętrze budynku Portowej Straży Pożarnej przy ul. Chrzanowskiego 15.

Koncepcję adaptacji pomieszczeń przedstawiono na rysunkach 7 i 8.

3.1.Wymagania infrastrukturalne.

Budynek znajduje się na terenie położonym w Gdyni przy ul. Bernarda Chrzanowskiego 15.

Pomieszczenia wyznaczone do remontu znajdują się w części biurowej budynku, na jego 2 piętrze, od strony południowej.

Pomieszczenia biurowe należy przystosować do pełnienia funkcji całodobowego monitoringu

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

budynków i terenów Zarządu Morskiego Portu Gdynia S.A. za pomocą zintegrowanego elektronicznego systemu zabezpieczeń.

W tym celu należy wydzielić pomieszczenie techniczne z jednego z pokoi biurowych na cele serwerowni oraz jadalni dla personelu.

- pow. użytkowa - 38,28m2,
- kubatura – 95,68 m3,
- wysokość pomieszczeń: - 2,5m.
- wysokość budynku: - ~10m.

Infrastruktura niezbędna do użytkowania pomieszczeń to istniejące w budynku:

- instalacje elektro-energetyczne,
- instalacje alarmowe,
- instalacja wodociągowa,
- instalacja kanalizacji sanitarnej,
- instalacja grzewcza,
- instalacja teletechniczna.
- instalacja wentylacji grawitacyjnej.

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

Projektowane pomieszczenia należy niezbędnie wyposażyć w klimatyzację, a w szczególności pokój 24h dozoru oraz nowe pomieszczenie serwerowni. Klimatyzatory będą zainstalowane w pomieszczeniach, centrale na dachu budynku. Pozostałe instalacje, a w szczególności instalacje niskoprądowe i teletechniczne należy wymienić na nowe.

Ewakuacja z pomieszczeń biurowych na 2 piętrze prowadzi poprzez korytarz i istniejącą klatkę schodową bezpośrednio na zewnątrz budynku.

Na poziomie 2 piętra znajduje się zespół sanitarny spełniający potrzeby higieniczno - sanitarne dla osób przebywających na tej kondygnacji.

Na potrzeby Centrum należy wykorzystać istniejącą instalację zasilania gwarantowanego, którą należy uzupełnić o stacjonarny agregat prądotwórczy. Dla zapewnienia podtrzymania pracy urządzeń teleinformatycznych przez czas niezbędny dla uruchomienia agregatu, w szafie serwerowej zostaną zastosowane UPS-y.

Propozycja zagospodarowania pomieszczeń – rys. 7 i 8. Wejście do Centrum oraz Serwerowni należy wyposażyć w dwustronną Kontrolę Dostępu a Serwerownię w system alarmowy.

Na rysunku 4 pokazano propozycję rozmieszczenia urządzeń kontroli dostępu, systemu alarmowego, gniazd LAN, interkomów.

Na rysunku 5 pokazano propozycję zagospodarowania szafy komputerowej systemowej.

Do łączności bezpośredniej pracowników odpowiedzialnych za bezpieczeństwo przewidziano system interkomowy. Interkomy połączą pracowników Centrum Monitoringu, Dyspozytora Portu, Posterunek alarmowy PSP oraz wejście do Centrum. Schemat pokazano na rysunku 6.

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

3.2.Wytyczne projektowe dla poziomów integracji podsystemów

Celem zastosowania systemu integrującego będzie dostarczenie jednolitej i neutralnej platformy informatycznej pozwalającej na wizualizację, obsługę, analizę działania, wsparcie operatorów stacjonarnych oraz mobilnych.

Schemat ideowy pokazano na rys. 1.

3.2.1. Integracja z systemem kontroli dostępu

W systemie muszą zostać przedstawiane stany przejść, a także czujników zamknięcia drzwi, czytników i przycisków w miejscach ich lokalizacji na planach sytuacyjnych (architektonicznych) oraz na schematach zbiorczych. Operator musi otrzymać nie tylko informacje o stanie urządzeń systemu kontroli dostępu, ale także informacje o numerze identyfikatora osobistego. Z poziomu systemu operator musi mieć możliwość sterowania drzwiami kontroli dostępu np. otworzyć na czas określony, odtworzyć na stałe, zablokować drzwi. Dla każdych drzwi z czytnikami i przyciskami ma być zdefiniowana procedura działania, plan sytuacyjny. Sygnały z systemu kontroli dostępu poprzez zdefiniowanie automatycznych procedur działania i automatycznych sterowań muszą mieć możliwość wywoływania działań innych zintegrowanych systemów np. przyłożenie karty do czytnika powoduje, że w systemie pokazywane jest zdjęcie danej osoby, a następnie dzięki integracji z systemem CCTV na monitorze wywoływany jest obraz z najbliższej kamery powiązanej z danym czujnikiem. System Kontroli dostępu musi pracować (współdzielić) na tej samej bazie danych co system integrujący, zapewniając spójną analizę zdarzeń i korelowanie z innymi systemami. Z poziomu integratora musi być możliwe nadawanie i edycja uprawnień użytkowników, administracja i raportowanie.

Integracja umożliwi nadzorowanie następujących stanów systemu KD:

- stany kontrolerów,
- stany wszystkich wejść cyfrowych w kontrolerach (spoczynek, alarm),
- stany wszystkich przekaźników w kontrolerach (wyłączony, włączony),
- stany logiczne drzwi (otwarte, otwarte na stałe, zamknięte, zablokowane),
- alarmy drzwi (drzwi za długo otwarte, drzwi otwarte bez autoryzacji),
- stany logiczne czytników (aktywny, zablokowany).
- próba użycia nieważnej lub nieznanej karty o danym numerze,
- próba podwójnego wejścia przy pomocy karty o danym numerze,
- użycie aktywnej karty o danym numerze.

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

Integracja umożliwi następujące sterowanie systemem KD:

- wysterowanie dowolnego przekaźnika w dowolnym kontrolerze na określony czas lub na stałe,
- zezwolenie na jednorazowe wejście,
- otwarcie drzwi na stałe,
- zablokowanie drzwi,
- zablokowanie czytnika.

3.2.2. Integracja z systemem monitoringu wizyjnego

W systemie integrującym, wizualizowane zostaną kamery, monitory oraz wejścia/wyjścia alarmowe kamer w miejscach ich instalacji na planach sytuacyjnych oraz na planszach zbiorczych. Specjalny moduł sterowania video pozwali na dowolne przełączanie kamer i monitorów, sterowanie kamerami obrotowymi, zmianę ostrości obrazu i przybliżenia, komponowaniem oraz zapisywaniem układów na monitorach oraz ustawianiem presetów na kamerach obrotowych. W systemie zarządzania zostaną utworzone wirtualne powiązania kamer z pozostałymi systemami budynkowymi miedzy innymi KD, SSWIN, SSP, których zadziałanie spowoduje przełączenie kamery na wybrany monitor alarmowy, wykonanie zdjęcia z danej kamery oraz uruchomienia nagrywania. W systemie zarządzani zdefiniowany zostanie monitor alarmowy, który jest specjalnie dedykowany do wyświetlania obrazów z kamer, gdy elementy wykonawcze zintegrowanych systemów zgłoszą meldunek (alarm, zakłócenie, uszkodzenie itd.). Operator będzie mógł również przełączać obrazy z kamer poprzez kliknięcie np. na piktogramy kamer umieszczone na planach sytuacyjnych (architektonicznych).

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

Integracja umożliwi nadzorowanie następujących stanów systemu CCTV:

- stanu krosownicy
- stanu wejść (włączony, wyłączony , awaria, praca)
- stanu wyjść (aktywne, nie aktywne , włączony, wyłączony , awaria, praca)
- stanu kamer (awaria , praca , wymagana konserwacja, aktywna, nie aktywna, stan oświetlenia kamery, włączona, wyłączona, nagrywanie)
- monitory (aktywny, nie aktywny , wyświetla sekwencję, połączenie alarmowe, alarm, spoczynek, praca);
- rejestratory (awaria, praca, do rejestratora jest przełączona kamera, rejestrator nagrywa)
- odtwarzacz (awaria, praca , odtwarzacz jest (stop, odtwarzanie, pauza), przewijanie w przód, przewijanie wstecz, odtwarzanie wstecz)

Integracja umożliwi następujące sterowanie systemem CCTV:

- wyjścia (włącz, wyłącz)
- stanu kamer (praca, alarm testowy, zazbrojenie czujnika kamery, włączenie, wyłączenie, włączenie oświetlenia kamery, sterownie kamerą obrotowa, ustawianie presetów, wybór presetu, jaśniej, ciemniej , zoom + zoom -, ustawienie ostrości, ustawienie ogniskowej na zbliżenie lub obraz szerokokątny)
- monitory (aktywny, nie aktywny, praca)
- rejestratory (przełączenie kamery, uruchomienie nagrania ze stemplem czasu, uruchomianie nagranie ze stemplem zdarzenie, awaria, praca)
- odtwarzacz (sterowanie odtwarzaniem: stop, pauza, wstecz, przewijanie wstecz , w przód, odtworzenie nagranie ze stempla czasu lub zdarzenia)

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

3.2.3. Integracja z systemem sygnalizacji pożaru,

W systemie zarządzania elementy detekcyjne i wykonawcze przedstawiane są, w miejscach ich zainstalowania, na planach sytuacyjnych oraz na planszach zbiorczych. Dla każdego elementu definiowane są procedury działań i określane szczegółowe plany sytuacyjne. Sygnały przesyłane przez System Sygnalizacji Pożaru mogą wywoływać zdefiniowane, automatyczne i ręczne procedury działań. Z poziomu komputera, operator będzie miał możliwość wykonywania czynności zbliżonych do obsługi centrali z poziomu wbudowanego pulpitu takie jak blokowanie elementów liniowych , potwierdzania oraz kasowanie fałszywych alarmów pożarowych. Poprzez moduły wykonawcze oraz sterujące centrali SSP będą monitorowane wszystkie urządzenia biorące udział w scenariuszu pożarowym. W systemie zostaną stworzone plansze odzwierciedlające matrycę sterowania dla poszczególnych stref budynków. Zapewni to możliwość kontrolowania sprawności wszystkich urządzeń oraz zapewni poprawność wykonania scenariuszy pożarowych na wypadek zaistnienia zdarzenia pożarowego.

Integracja umożliwi następujące sterowanie systemem SSP :

- Wyciszanie wewnętrznego sygnalizatora dźwiękowego.
- Wyłączanie zewnętrznych sygnalizatorów dźwiękowych.
- Kasowanie alarmów.
- Odłączanie pojedynczych czujników lub ROP-ów.
- Ustawianie pojedynczych czujników lub ROP-ów w tryb kontroli.
- Odłączanie grup czujników lub ROP-ów.
- Ustawianie grup czujników lub ROP-ów tryb w kontroli.
- Odłączanie pętli.
- Odłączanie wyjścia.
- Odłączanie wejścia.

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

Integracja umożliwi nadzorowanie następujące elementów systemu SSP :

- Stanu akumulatora.
- Stanu zasilania z sieci 230VAC.
- Stanu poziomu dostępu do centrali.
- Stanu wewnętrznego sygnalizatora dźwiękowego.
- Stanu zewnętrznych sygnalizatorów dźwiękowych.
- Stanu drukarek wewnętrznej i zewnętrznej.
- Stanów wejść.
- Stanów wyjść.
- Stanów czujników i ROP-ów.
- Stanu pętli.

3.2.4. Integracja z systemem sygnalizacji włamania i napadu,

System sygnalizacji włamania i napadu zostanie zintegrowany poprzez dedykowany interfejs. W systemie zostanie wizualizowany stan każdego z czujników systemu SSWiN, zazbrojenie strefy, sygnały alarmowy itp. System umożliwi również zdalne zazbrojenie i rozbrojenia strefy, oraz podgląd sytuacji w pobliżu pomieszczenia objętego systemem SSWiN poprzez powiązanie obrazu z kamery CCTV do stref SSWiN. Sygnały z systemu SSWiN będą wizualizowane na planach architektonicznych obiektu oraz na zbiorczych planszach systemowych.

W systemie zarządzania elementy detekcyjne i wykonawcze przedstawiane są, w miejscach ich zainstalowania, na planach sytuacyjnych oraz na planszach zbiorczych. Dla każdego elementu definiowane są procedury działań i określane szczegółowe plany sytuacyjne. Sygnały przesyłane przez SSWiN mogą wywoływać zdefiniowane, automatyczne i ręczne procedury działań. Z poziomu komputera, operator będzie miał możliwość wykonywania czynności zbliżonych do obsługi centrali. Monitorowane będą wszystkie urządzenia biorące udział w scenariuszu pożarowym. W systemie zostaną stworzone plansze odzwierciedlające matrycę sterowania dla poszczególnych stref budynków. Zapewni to możliwość kontrolowania sprawności wszystkich urządzeń

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

Integracja umożliwi następujące sterowanie systemem SSWiN :

- Wyciszanie wewnętrznego sygnalizatora dźwiękowego.
- Wyłączanie zewnętrznych sygnalizatorów dźwiękowych.
- Kasowanie alarmów.
- Operowanie pojedynczymi czujnikami.
- Operowanie strefami włamaniowymi.

Integracja umożliwi nadzorowanie następujące elementów systemu SSWiN:

- Stanu akumulatora.
- Stanu zasilania z sieci 230VAC.
- Stanu poziomu dostępu do centrali.
- Stanu sygnalizatorów dźwiękowych.
- Stanów wejść.

3.2.5. Integracja z systemem ochrony obwodowej,

Istniejące systemy ochrony obwodowej są monitorowane jako stany elektryczne przy pomocy systemu sygnalizacji włamania i napadu. Statusy przyłączanych w przyszłości dodatkowych systemów będą wizualizowane na planach architektonicznych obiektu oraz na zbiorczych planszach systemowych.

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

3.3. Wytyczne projektowe dla części teletechnicznej

Pomieszczenie teletechniczne powinno być wyposażone w dwa stanowiska operatorów. Każde stanowisko ma być wyposażone w monitor, klawiaturę, myszkę podłączone zdalnie do komputera umieszczonego w szafie serwerowej w Serwerowni. Do wizualizacji całego systemu należy wykonać Videowall zbudowany z 4 monitorów, zainstalowanych naprzeciwko stanowisk dyspozytorów.

Stanowisko jednego z operatorów będzie wyposażone w pulpit odbierania sygnałów alarmowych SSWiN, przeniesiony z dotychczasowej lokalizacji.

Podobnie monitoring sygnałów alarmowych z central Sygnalizacji Pożaru, istniejący w pomieszczeniu Dyspozytora Portu, zostanie przeniesiony na Posterunek alarmowy PSP, zlokalizowany na parterze PSP. Schemat transmisji alarmów pokazano na rys. 2.

3.4.Wytyczne projektowe dotyczące punktów obsługi zdarzeń alarmowych

Efektem zakończenia proponowanych prac będzie sytuacja, w której w ZMPG pojawią się trzy ośrodki decyzyjne,

1. Punkt Alarmowy Portowej Straży pożarnej,
2. Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń (obecnie Centrum Monitorowania Alarmów)
3. Portowa Straż Pożarna.

Takie rozdział kompetencji wydaje się nie korzystny. W związku z tym, po konsultacja z przedstawicielami ZMPG oraz wizjach lokalnych, proponuje się przeniesienie Punktu alarmowego Portowej Straży Pożarnej do budynku PSP przy ulicy Chrzanowskiego 15. Decyzja ta nie niesie za sobą nadmiernych nakładów pracy i kosztów ze względu na istniejącą infrastrukturę SSP w budynku. W odpowiednim pomieszczeniu na parterze jest zdublowany Punkt alarmowy PSP, który utrzymywany jest w stanie gotowym do przejęcia obowiązków Punktu alarmowego PSP z ul. Rotterdamskiej.

W ramach realizacji koncepcji należy stworzyć Centrum Nadzoru Elektronicznych Systemów Zabezpieczeń. Po przeprowadzeniu wizji lokalnych zdecydowano się zaproponować budynek PSP przy ulicy Chrzanowskiego Lokalizacja ta ma szereg zalet. Najważniejsze z nich to:

- Na drugim piętrze budynku znajdują się trzy pomieszczenia, które postanowiono zaadoptować do potrzeb Centrum Nadzoru Elektronicznych Systemów Zabezpieczeń. Ich powierzchnia pozwala na wybudowanie serwerowni, części socjalnej i szatni.

Można również wygospodarować przestrzeń potrzebną do realizacji Centrum Nadzoru Elektronicznych Systemów Zabezpieczeń.

- Kubatura pomieszczeń zapewni możliwość obsługi zarówno przez pracownika ZMPG jak i również pracownika firmy ochroniarskiej.
- W budynku znajduje się węzeł pierścienia LAN, co zapewnia redundancję sieciową.
- W budynku jest przyłącze do zasilania agregatem.

Po konsultacji z przedstawicielami ZMPG i PSP jako miejsce docelowe CNESZ wskazać budynek PSP przy ul. Chrzanowskiego.

Dzięki tym działaniom W jednym budynku, względnej bliskości siebie będą funkcjonować wszystkie ośrodki decyzyjne, zarządzające bezpieczeństwem na terenie ZMPG. Ponadto należy pomieszczenie CNESZ, Punkt Alarmowy oraz Dyspozytora Portu połączyć należy systemem interkomowym, dającym najlepszą możliwość szybkiego bezpiecznego i wydzielonego połączenia.

3.5.Serwerownie

W serwerowni podstawowej przewidziano instalację szafy serwerowej z serwerami oprogramowania integrującego, interkomowego oraz komputerami operatorów i zasilaczami UPS. Wyposażenie w sprzęt komputerowy jest opisane w dalszej części opracowania. Serwerownię należy wyposażyć w klimatyzator.

Serwery redundantne powinny stanąć w pomieszczeniu zapewnionym przez Dział IT.

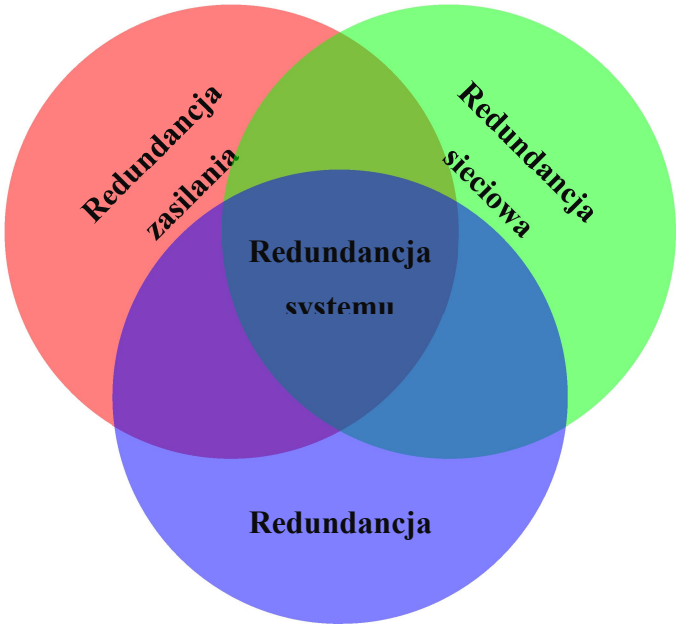
3.6. Redundancja

Istotną cechą integratora elektronicznych systemów zabezpieczeń powinna być nadmiarowość. Żeby osiągnąć maksymalnie duży stopień stabilności pracy systemu, redundancję systemową, należy spełnić trzy główne warunki:

1. Redundancja zasilania.
2. Redundancja sieciowa.
3. Redundancja oprogramowania.

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

Rysunek 1 Redundancja systemowa



Redundancja zasilania zapewnia prawidłowe działanie integratora w warunkach zaniku zasilania. Szczegóły zostały omówione w rozdziale 3.2.

Redundancja sieciowa zapewnić powinna alternatywną drogę połączenia pomiędzy serwerami (podstawowym i redundantnym) a klientami w Centrum nadzoru elektronicznych systemów zabezpieczeń. Żeby ją osiągnąć należy spełnić warunki przedstawione w rozdziale 3.5.

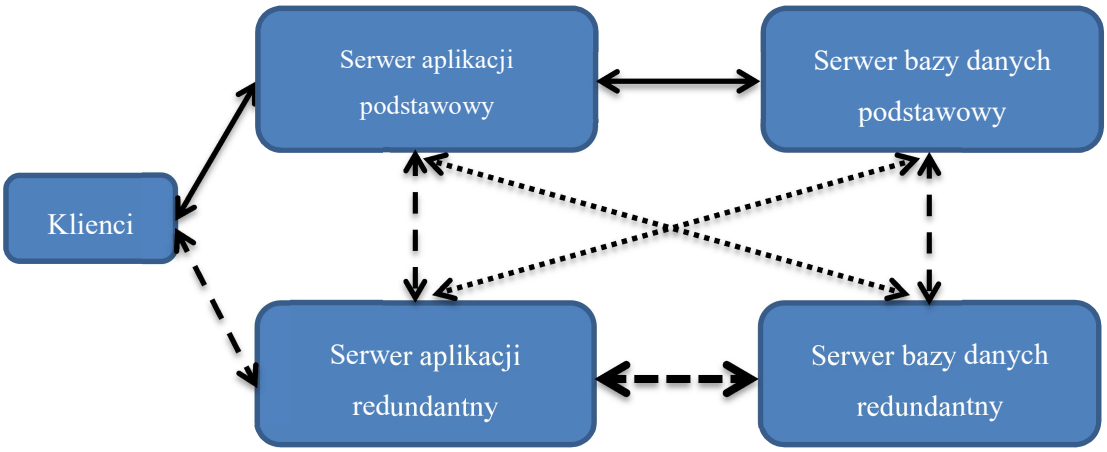
Redundancja oprogramowania zapewniona zostanie poprzez zastosowanie następującej konfiguracji:

- Serwer aplikacji, podstawowy,
- Serwer bazy danych, podstawowy,
- Serwer aplikacji, redundantny,
- Serwer bazy danych, redundantny.

Wytyczne projektowe dla Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń.

Poniższy schemat wyjaśnia w jaki sposób powinna odbywać się komunikacja pomiędzy poszczególnymi serwerami podczas pracy w trybie normalnym i awaryjnym:

Rysunek 2 Schemat działania redundancji softwarowej



W normalnym trybie pracy klienci komunikują się z serwerem aplikacji, który współpracuje z Serwerem bazy danych w kwestii uprawnień, zmian archiwizacji zdarzeń itp. Serwery redundantne sprawdzają „widoczność" swoich podstawowych odpowiedników, w regularnych odstępach czasu. Poprzez „widoczność" należy rozumieć prawidłowe działanie sieci LAN, hardware'u i software' u. W trakcie ich pracy aktualizują swoje ustawienia, bazę danych itp. Efektem takiego układu powinna być kopia zapasowa całego systemu, zarówno aplikacji, jak i bazy danych.

Cała komunikacja odbywa się za pośrednictwem sieci LAN (patrz rozdział 3.3 Wytyczne projektowe dla części teletechnicznej).

Wszystkie scenariusze pracy systemu powinny opierać się o działania autonomiczne i automatyczne tj. bez udziału użytkownika.

W normalnym trybie pracy klient komunikuje się z serwerem aplikacji. Serwer aplikacji w razie potrzeby odwołuje się, do serwera bazy danych. Układ taki zapewnia stabilną pracę systemu.

W przypadku awarii Serwera aplikacji, lub Serwera Bazy Danych, jego funkcję przejmuje odpowiedni serwer redundantny. Należy pamiętać, że czynność ta może zabrać nawet parę minut. Po przełączeniu układu system powinien działać stabilnie.

W przypadku awarii Serwera Aplikacji i Serwera Bazy Danych ich funkcje przejmują serwery redundantne. Należy pamiętać, że czynność ta może zabrać nawet parę minut. Po przełączeniu układu system powinien działać stabilnie.

Powrót do podstawowych ustawień odbywa się automatycznie po odzyskania połączenia pomiędzy częścią redundantną i podstawową. Bazy danych powinny się zsynchronizować.

4. Topologia sieci.

Łączność Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń z urządzeniami będącymi źródłami danych dla Centrum zapewni dedykowana sieć komputerowa , jej topologia będzie powielać kształt topologii funkcjonującej w Porcie Gdynia. Należy zapewnić odseparowanie tej sieci od reszty sieci przedsiębiorstwa. Główny szkielet sieci stanowią następujące węzły sieciowe:

1. Kwiatkowskiego 60A 1-IT
2. Indyjska 13
3. Rotterdamska 9
4. Polska 17
5. Warsztatowa 4

W węzłach tych należy zainstalować przełączniki sieciowe z portami SFP i Gigabit Ethernet. Połączenie pomiędzy tymi węzłami zrealizowane będzie przy pomocy udostępnionych przez Port Gdynia jednomodowych włókien światłowodowych. Ponadto pomiędzy węzłami „Kwiatkowskiego 60A 1 IT" a „Warsztatowa 4" zapewnione jest dodatkowe połączenie światłowodowe, dzięki któremu można stworzyć sieć w topologii pierścienia. Obecnie nie jest możliwe zapewnienie po parze włókien pomiędzy wszystkimi przełącznikami tworzącymi główny szkielet sieci, dlatego też konieczne będzie poprowadzenie nowego kabla światłowodowego pomiędzy węzłami „Kwiatkowskiego 60 A 1-IT" a „Indyjska 13". Przyjętym standardem dla takiej rozbudowy jest dodanie kabla 96J SMF. Topologię rozbudowy sieci pokazano na rys. 3. Dodatkowo przewidzieć należy odpowiednią ilość licencji do systemu zarządzającego infrastrukturą sieciową: HPE Intelligent Management Center

Topologia sieci.

Do głównych węzłów sieciowych przyłączone będą przełączniki sieciowe zapewniające dostęp do sieci w poszczególnych lokalizacjach, tj.:

1. Wiśniewskiego 31
2. W2 Kontenerowa 6
3. Magazyn 11 Kontenerowa
4. Magazyn 12 Kontenerowa 27
5. GPKW Kwiatkowskiego 60
6. Kwiatkowskiego 60 A1 Portiernia
7. Terminal promowy Kwiatkowskiego 60
8. Wiśniewskiego 23 (połącznie kablami miedzianymi)
9. Zbiorniki Demela (połączenie poprzez dzierżawioną linię „Orange”)
10. Al. Solidarności 1c
11. Indyjska 2
12. Indyjska 1 BTZ
13. Indyjska 1 SAR
14. Polska 43 V piętro
15. Polska 13A
16. Polska 13
17. Magazyn K
18. Chrzanowskiego 15

5. Obsada stanowiskowa Centrum Zarządzania Elektronicznych Systemów Zabezpieczeń

Centrum w swoim projektowanym kształcie i przy założonych funkcjach przewidziano dla dwuosobowej obsady. Jednym z pracowników jest etatowy pracownik ZMPG w roli operatora Centrum, drugim jest pracownik firmy Ochrony Osób i Mienia wyłonionej przez ZMPG w odrębnym postępowaniu. Pracownik firmy OOiM winien być kwalifikowanym pracownikiem Ochrony Fizycznej z uprawnieniem do monitorowania sygnałów alarmowych a także legitymowania i/lub interwencji w sytuacjach krytycznych (uprawnienia pracowników ochrony w czasie pełnienia obowiązków służbowych reguluje rozdział 6 (art. 36-42) ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia -tekst jednolity Dz.U. 2014 poz. 1099). Pracownik taki ma prawo używać broni służbowej i środków przymusu bezpośredniego.

Pracownicy pracować będą w systemie zmianowym 12 godzin służby- 24 godziny odpoczynku. Zmusza to przełożonych do utrzymywania 3+1 zespołów obsady.

Do bezpośrednich obowiązków załogi należy nadzorowanie pracy systemów zarządzania Elektronicznymi Systemami Zabezpieczeń ZMPG, dozorowanie sygnałów alarmowych, podejmowanie działań zgodnych z opracowaną przez przełożonych procedurą dla każdego z możliwych zagrożeń jak również raportowanie przebiegu służby i informowanie przełożonych o każdej nieprzewidzianej sytuacji. Każdy z zatrudnionych winien ukończyć kurs szkolenia stanowiskowego dla operatora Centrum Zarządzania ESZ ZMPG.

Dodatkowo: należy przestrzegać zapisów ROZPORZĄDZENIA Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy.

6. Cykl życia produktu

6.1. Określenie warunków zakończenia życia technologicznego produktów

W przypadku elektronicznych systemów zabezpieczeń, kres życia technicznego danego produktu należy rozumieć taki moment, w którym:

1. Urządzenia zbliżają się do granicy poprawności działania wykazanej w kartach katalogowych (np. liczby przełączeń przekaźników, możliwości zapisu na dyskach itp.).
2. System generuje dużą liczbę alarmów fałszywych.
3. Efekty pracy systemu znacząco odbiegają od osiąganych w momencie instalacji (np. w CCTV brak kolorów).

Cykl życia produktu

4. Elementy systemu posiadają zwiększoną awaryjność.
5. Ograniczony dostęp do części zamiennych.
6. Zwiększone ryzyko ponoszenia kosztów eksploatacyjnych.
7. Brak możliwości rozwoju.

Korzystając z tych wytycznych dokonano przeglądu systemów i określono te z nich, które zbliżają się do osiągnięcia, lub osiągnęły kres życia technicznego. Listę zawarto w rozdziale 6.2 Określenie podsystemów wymagających modernizacji.

6.2.Określenie podsystemów wymagających modernizacji

Niniejszy rozdział przedstawia spis podsystemów, które należy zmodernizować w związku z zbliżeniem, lub osiągnięciem kresu życia technologicznego, wybrany integrator nie obsługuje danego formatu danych, lub dany podsystem, lub jego składowa nie dają możliwości integracji.

Tabela 6 Podsystemy wymagające modernizacji

L.P.	Podsystem	Lokalizacja	Przyczyna modernizacji
1	Roconet / SSWiN	Rotterdamska 9	kraniec życia technicznego
2	UTC / CCTV	Rotterdamska 9	kraniec życia technicznego
3	Roconet / SSWiN	Węglowa 8	kraniec życia technicznego
4	Roconet / SSWiN	Rotterdamska 7	kraniec życia technicznego
5			

II. PROGRAM FUNKCJONALNO UŻYTKOWY

Nazwa zadania:

Zaprojektowanie, wybudowanie i uruchomienie Integracji Elektronicznych Systemów Zabezpieczeń w obiektach Zarządu Morskiego Portu Gdynia.

Podmiotem zadania:

Zarząd Morskiego Portu Gdynia.

Lokalizacja zadania:

Elektroniczne Systemy Zabezpieczeń, oraz towarzysząca infrastruktura teleinformatyczna w następujących lokalizacjach:

1. Kwiatkowskiego 60A 1-IT
2. Indyjska 13
3. Rotterdamska 9
4. Polska 17
5. Warsztatowa 4
6. Wiśniewskiego 31
7. W2 Kontenerowa 6
8. Magazyn 11 Kontenerowa
9. Magazyn 12 Kontenerowa 27
10. GPKW Kwiatkowskiego 60
11. Kwiatkowskiego 60 A1 Portiernia
12. Terminal promowy Kwiatkowskiego 60
13. Wiśniewskiego 23 (połącznie kablami miedzianymi)
14. Zbiorniki Demela (połączenie poprzez dzierżawioną linię „Orange”)
15. Al. Solidarności 1c
16. Indyjska 2
17. Indyjska 1 BTZ
18. Indyjska 1 SAR
19. Polska 43 V piętro
20. Polska 13A
21. Polska 13
22. Magazyn K
23. Chrzanowskiego 15
24. Rotterdamska 13

25. Celna 5
26. Wiśniewskiego 23
27. Demela
28. Węglowa 8
29. Rotterdamska 7
30. Czechosłowacka 5
31. Chrzanowskiego 17

Przedmiot zamówienia obejmuje wykonanie w obiektach ZMPG następujących prac:

1. Zaprojektowanie, wybudowanie i uruchomienie systemu Integracji Elektronicznych Systemów Zabezpieczeń zbierających informacje z wymienionych lokalizacji.
2. Zaprojektowanie, wykonanie prac remontowo - dostosowawczych w Centrum Monitoringu.
3. Zaprojektowanie wybudowanie i uruchomienie infrastruktury teleinformatycznej.

Dla każdej lokalizacji objętej projektem należy:

- Opracować wielobranżowy projekt budowlany i wykonawczy w zakresie umożliwiającym wykonanie całości robót jak i uzyskanie decyzji administracyjnych wymaganych Prawem Budowlanym, jeżeli będzie ona wymagana
- Zrealizować, na podstawie opracowanej dokumentacji, wszystkie roboty w poszczególnych branżach.
- Opracować harmonogram obowiązkowych prac eksploatacyjnych, utrzymaniowych i serwisowych zawierający wszelkie prace i zabiegi konserwacyjne, regulacyjne i kontrolne zamykające się w cyklu rocznym. Wykaz czynności serwisowych i utrzymaniowych o cyku powyżej roku Wykonawca przedstawi w odrębnym harmonogramie.

W ramach zamówienia, Wykonawca jest zobowiązany do uwzględnienia wszystkich zależności wynikających z infrastruktury należącej do innych podmiotów.

Wykonawca zobowiązany jest do pozyskania i przekazania zamawiającemu licencji bez ograniczeń czasowych (o ile licencje będą wymagane) potrzebnych do realizacji wszystkich systemów, sieci, instalacji itd..

Dalej w tekście przedstawiono szczegółowy opis i wymagania dotyczące podsystemów Integratora

1. Zakres rzeczowy przedmiotu zamówienia

W zakres realizacji przedmiotu zamówienia wchodzi wykonanie dokumentacji projektowej Integracji Elektronicznych Systemów Zabezpieczeń wraz z budową systemu a w szczególności:

1. Wykonanie kompletnej dokumentacji projektowej dla zbudowania Integracji Elektronicznych Systemów Zabezpieczeń wraz z adaptacją, przebudową istniejących pomieszczeń i budową nowych przejść, wyodrębnieniem i przygotowaniem w Centrum Monitoringu serwerowni, części socjalnej, pokoju monitoringu i szatni, składającej się z projektów branżowych projektów wykonawczych, specyfikacji technicznych wykonania i odbioru robót oraz uzyskanie potrzebnych zezwoleń i uzgodnień a także sprawowanie nadzorów autorskich.
2. Wybudowanie, adaptacja budowlana przejść, wyposażenie w przegrody (bariery) fizyczne
3. Dostawa, montaż i uruchomienie urządzeń sieciowych na potrzeby Integracji.,
4. Wybudowanie brakujących odcinków sieci światłowodowych.
5. Wykonanie niezbędnych prac kablowych, instalacyjnych
6. Wykonanie przyłączy do sieci informatycznej
7. Dostawa montaż i uruchomienie komputerowych stanowisk klienckich dla Zintegrowanego Systemu Zabezpieczeń Elektronicznych dla Centrum monitoringu.
8. Dostawa montaż i uruchomienie serwera aplikacji i serwera zapasowego
9. Przeprowadzenie prób i badań wymaganych od systemu integratora, oraz przygotowanie dokumentów związanych z oddaniem przedmiotu w użytkowanie.
10. Uruchomienie systemu i przekazanie do eksploatacji.
11. Szkolenia pracowników w zakresie obsługi systemu.
12. Dostarczenie, zainstalowanie i uruchomienie pozostałych elementów systemu, wynikających z koncepcji budowy Integratora.
13. Uzyskanie niezbędnych uzgodnień z gestorami sieci i urządzeń, dotyczącymi przebiegu przyłącza i sposobu ich wykonania.
14. Uzyskanie niezbędnych uzgodnień umożliwiających realizację przedmiotu zamówienia (np. pozwolenie na zajęcie pasa drogowego).
15. Dokumentację projektową oraz specyfikacje techniczne wykonania i odbioru robót budowlanych należy wykonać zgodnie z Rozporządzeniem Ministra Infrastruktury z dn.2.09.2004, Dz.U. z dn. 16.09.2004 w zakresie i ilości niezbędnej do uzyskania wymaganych uzgodnień i pozwolenia na budowę, zgodnie z:

- wymaganiami funkcjonalnymi i technicznymi określonymi przez Zamawiającego,
- wymaganymi opiniami i sprawdzeniami rozwiązań projektowych w zakresie wynikającym z obowiązujących przepisów, a w szczególności:
    - ustawą z dnia 07.07.1994r. Prawo budowlane (j.t. Dz.U. z 2003r. Nr 207, poz. 2016 z późn. zm.),
    - ustawą z dnia 30.08. 2002r. o systemie oceny zgodności (Dz. U. Nr 204, poz. 2087 ze zm.),
    - rozporządzeniem Prezesa Rady Ministrów z 25.02.1999r. w sprawie podstawowych wymagań bezpieczeństwa i sieci teleinformatycznych (Dz. U. Nr 18, poz. 162),
    - rozporządzeniem Ministra Pracy i Polityki Socjalnej z 01.12.1998r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz. U. Nr 148, poz. 973),
    - Polską normą dotyczącą systemów kontroli dostępu PN-EN 50133-1.
    - Ustawą z 16 lipca 2004 Prawo Telekomunikacyjne (Dz.U. Nr 171 poz. 1800.

16. Ponadto Zamawiający otrzyma dodatkowo trzy komplety dokumentacji w wersji papierowej oraz jeden komplet w wersji elektronicznej wraz z kompletem wszystkich uzyskanych uzgodnień i pozwoleń. Po wykonaniu przedmiotu zamówienia Wykonawca dostarczy komplet dokumentacji powykonawczej ze wszystkimi uzgodnieniami i pozwoleniami w oryginale.
17. Na etapie projektowania wymagana jest akceptacja rozwiązań funkcjonalno - technicznych oraz materiałowych przez Zamawiającego przed złożeniem wniosku o uzyskanie pozwolenia na budowę oraz na etapie wykonywania branżowych projektów wykonawczych.

2. Wymagania techniczne i funkcjonalne

2.1. Urządzenia

Minimalne parametry sprzętowe głównego i zapasowego serwera zintegrowanego systemu zabezpieczeń technicznych:

- 2 x Procesor Intel Xeon E5-2609 v4 1.7GHz,20M Cache,6.4GT/s QPI,8C/8T (85W) Max Mem 1866MHz
- Obudowa pozwalająca na zamontowanie do 8 dysków twardych 3.5"
- 16 GB pamięci RDIMM, 2400MT/s, w module jednobankowym, szerokość magistrali x8
- zintegrowany kontroler dostępu zdalnego w wersji Enterprise
- 4 dyski 300GB 15K RPM SAS 2.5in Hot-plug 3.5 cala HYB CARR
- zintegrowany kontroler RAID, 1GB pamięci podręcznej
- DVD+/-RW napęd SATA wewnętrzny
- Dual, Hot-plug, Redundant Power Supply (1+1), 750W
- 2 x Europejski przewód zasilający 230V
- Wbudowana karta LAN 1GBE (dwuportowa dla obudów typu tower, czteroportowa dla szaf serwerowych i modułów kasetowych)
- Windows Server 2016 Standard Edition, zainstalowany fabrycznie, z nośnikami, 2 procesory, 2 maszyny wirtualne, 16 CAL
- Gwarancja podstawowa
- 3Yr Basic Warranty - Next Business Day - Minimum Warranty
- 5Yr ProSupport and 4hr Mission Critical
- 5Yr Data Protection - Keep Your Hard Drive

Wymagania techniczne i funkcjonalne

Minimalna konfiguracja Stacji Roboczej i komputera obsługującego ścianę wizyjną:

- Procesor Intel® Xeon® E3-1270 v5 (3.60 GHz, 4 Rdzenie, 8MB Cache, DMI 8.00GT/s, 80W)
- Obudowa typu Tower 3420 Up to 92% efficient 240W Chassis, v2
- 8GB (2x4GB, 2400MHz, DDR4, ECC, UDIMM)
- 3.5" 500GB 7200rpm SATA HDD
- Zintegrowany kontroler Intel, SATA 6Gb/s RAID 0/1/5 (4 porty)
- Radiator procesora 65 W do obudowy typu SFF
- DVD-/+RW 8x
- przewód zasilający Euro
- karta graficzna AMD FirePro™ W4100 (2GB, 4 x MiniDP, 50 W)Optical Mouse MS116 Black
- Monitor 24” LED LCD FHD przeznaczony do pracy ciągłej
- Multimedia Keyboard KB216 Black (US International - QWERTY)
- Karta dźwiękowa
- Usługa SupportAssist
- Pojemność woluminu rozruchowego lub pamięci masowej mniejsza niż 2 TB
- Windows 10 Pro (64-bitowy) wielojęzyczny, wersja angielska, czeska, węgierska, polska, słowacka
- Windows 10 Pro OS Recovery 64bit - DVD
- Microsoft Office - 30-dniowa wersja próbna, wyklucza licencję pakietu Office
- Base Warranty
- 1Yr Basic Warranty - Next Business Day - Minimum Warranty
- 3Yr Basic Warranty - Next Business Day
- 3Yr Data Protection - Keep Your Hard Drive

SIEĆ KOMPUTEROWA

Wymagania dotyczące przełączników sieciowych:

- Praca w warstwie L3
- obsługa jakości serwisu (QoS)
- Obsługa Multicast
- Zarządzanie przez stronę www
- Liczba portów (gniazd) RJ-45 Ethernet: 24
- Podstawowe przełączania Ethernet RJ-45 porty typ: Gigabit Ethernet (10/100/1000)
- Liczba zainstalowanych modułów SFP SFP: 4
- Port konsoli RJ-45
- Technologia okablowania Copper Ethernet: 10BASE-T,100BASE-TX,1000BASE-T
- Standardy komunikacyjne: IEEE 802.3,IEEE 802.3ab,IEEE 802.3u
- Pełny dupleks
- Agregator połączenia
- Limit częstotliwości
- Serwer DHCP
- przekierowywanie IP
- IGMP snooping
- Automatyczne MDI/MDI-X MDI
- Protokół drzewa rozpinającego
- Pozycja routingu: 10000
- Obsługa sieci VLAN
- Auto-sensing
- Przekazanie (audycja) Danych
- Przepustowość rutowania/przełączania Ilość przesłanych danych na sekundę: 56 Gbit/s
- Przepustowość: 41.7 Mpps
- Wielkość tabeli adresów: 32768 wejścia
- Latency (1 Gbps): 3.8 µs
- Zgodny z Jumbo Frames
- Lista kontrolna dostępu (ACL)

- obsługuje SSH/SSL
- Rozmiar układu 1U
- Możliwość Stackowania
- Taktowanie procesora : 1016 Mhz
- Pojemność pamięci wewnętrznej Ilość pamięci: 1024 MB
- Typ pamięci: DDR3 SDRAM
- Napięcie wejściowe AC: 100-240 V
- Pobór mocy: 19.5 W
- Maksymalne zużycie mocy : 29.3 W
- Zakres temperatur (eksploatacja) : 0 - 45 °C
- Zakres wilgotności względnej: 15 - 95 %
- Emisja ciepła: 100 BTU/godz

Wymagania techniczne i funkcjonalne

KONTROLA DOSTĘPU

Do obsługi kontroli dostępu należy przewidzieć kontrolery systemu Unicard. Czytniki kart zbliżeniowych powinny współpracować z kontrolerami firmy Unicard i mieć możliwość odczytu kart Mifare Classic / Mifare Plus. System powinien być oparty na kontrolerach przejść obsługujących dwa przejścia wyposażone w dwa czytniki kart. Proponuje się, by każdy kontroler obsługiwał wyłącznie jedno przejście kontroli dostępu. Kontrolery powinny być wyposażone w zasilanie awaryjne w postaci akumulatora 12V 7Ah. Przewiduje się podłączenie kontrolerów do sieci IP by mogły być nadzorowane przez dotychczas użytkowany system UniKD.

Elektryczne drzwiowe urządzenia wykonawcze:

- Elektryczne drzwiowe urządzenia blokujące (rygle/zwory/zamki) wyszczególnione poniżej muszą być zasilane z osobnego źródła, podtrzymywanego bateryjnie. Źródło powinno być wyposażone w bezpiecznik i mieć wystarczającą wydajność dla zasilenia przynajmniej ośmiu (8) urządzeń drzwiowych. Zastosowane akumulatory muszą zapewnić pracę bez głównego zasilania przez 48 godzin. Urządzenie powinno być wyposażone w styki (normalnie zwarte) do podłączenia sygnału alarmu pożarowego.
- Wszystkie urządzenia blokujące mają pozostawać otwarte przy braku zasilania (fail-safe), o ile nie ma innych zaleceń Projektanta. Wszystkie urządzenia blokujące mają pozostawać zamknięte w przypadku braku zasilania lub alarmu pożarowego, o ile spełnione są wymagania dla bezpiecznej ewakuacji, zgodnie z przepisami prawa budowlanego.
- Styki między dostawcami urządzeń wykrywających alarm pożarowy, stałych urządzeń gaśniczych a dostawcą urządzeń wykonawczych muszą być uzgodnione i zaakceptowane przez Użytkownika.

Wymagania techniczne i funkcjonalne

Konfiguracja osprzętu drzwiowego:

- Drzwi wymagające kontroli dostępu muszą być wyposażone w ewakuacyjny przycisk wyjścia, służący do awaryjnego otwarcia drzwi w sytuacjach zagrożenia życia. Przycisk musi być wyposażony w dwubiegunowy styk przełączny, służący do wysłania polecenia otwórz drzwi do kontrolera oraz do bezwarunkowego przerwania obwodu blokującego otwarcie drzwi.
- Kontroler dostępu muszą być wyposażone w wejście dla monostabilnego przycisk wyjścia, wyposażony w jednobiegunowy styk przełączny, z wyborem stanu normalnego (zamknięte/otwarte – NC/NO). Naciśnięcie przycisku jest dla kontrolera żądaniem otwarcia drzwi.

Urządzenia wykrywające włamanie lub napad:

Drzwiowe czujniki magnetyczne:

- Wpuszczane w ościeżnicę czujniki magnetyczne muszą być zamontowane we wszystkich drzwiach wymagających kontroli dostępu i/lub sygnalizacji włamania i napadu. Na drzwiach dwuskrzydłowych należy zamontować dwa czujniki, po jednym na skrzydło. Kolor należy dopasować do kolorystyki drzwi/ościeżnic.
- W miejscach, gdzie niemożliwe jest ukrycie okablowania w ościeżnicy lub ścianie, czujniki drzwiowe wpuszczane muszą być zastąpione nawierzchniowymi, a okablowanie prowadzone w pancerzu utrudniającym sabotaż.
- Do bram przesuwnych należy zastosować czujniki specjalnie wzmocnione, a okablowanie prowadzone w pancerzu utrudniającym sabotaż.
- Wszystkie czujniki powinny być okablowane bez rozszyć do najbliższego kontrolera lub do specjalnej puszki połączeniowej.
- Wszystkie czujniki drzwi powinny być zasilane z jednego, centralnego źródła 12VDC w obrębie lokalizacji.
- powinno minimalizować ryzyko fałszywego alarmu spowodowanego np. warunkami oświetlenia lub pogody.
- Wszystkie czujniki powinny być okablowane bez rozszyć do najbliższego kontrolera lub do specjalnej puszki połączeniowej.

Wymagania techniczne i funkcjonalne

System Interkomowy:

Wymagania dotyczące interkomów nabiurkowych:

- Cyfrowy serwer interkomowy IP (funkcje głosowe, wideo, wskazywania i sterowania).
- Integracja pozostałych serwerów poprzez złącze Ethernet oraz V24 z własnym konwerterem protokołu
- Obudowa centrali oraz technologia połączeniowa opracowana pod kątem wymogów szaf rakowych 19".
- sterowanie przy użyciu mikroprocesora, konstrukcja o dużej gęstości, wyrób SMD, programowanie obiektowe. Dla wszystkich rodzajów stacji interkomowych (IP. 2 żyłowych oraz 4-żyłowych).
- Sieciowanie cyfrowe poprzez IP, 2-żyłowe lub 4-żyłowe linie, E1 lub ISDN.
- Zintegrowane funkcje na potrzeby sterowania drzwiami/ bramami, konferencji oraz pulpitów sterowania centralą.
- Integracja wideo poprzez Plug&Play.
- Rozbudowywany od 2 do maks. 5 760 abonentów bez ograniczeń (do 30 tys. abonentów z ograniczeniami).
- Zakres częstotliwości audio: 200 – 16 000 Hz
- Zniekształcenie audio: Poniżej 0,9%
- Zakres temperatury roboczej: Od 0°C do +50°C
- Zakres temperatury przechowywania: Od –30°C do +60°C
- Wilgotność względna: 20% do 80%

Konfiguracja przyjazna użytkownikowi za pomocą dołączonego oprogramowania komputerowego.

Wymagania dotyczące interkomów nabiurkowych:

- Technologia IP z wbudowanym DSP
- Standardowa klawiatura oraz przyciski funkcyjne
- Podświetlany, graficzny wyświetlacz LCD (8 linii po 14 znaków każda)
- Obsługa standardu OpenDuplex ® zapewniający naturalną komunikację bez użycia rąk
- Wielofunkcyjna dioda LED, zapewniająca wizualne wskazówki oraz informacje
- Wzmacniacz 2,5 W klasy "D" (1.5 W mocy wyjściowej w przypadku wbudowanego głośnika)

- Wyposażenie w dodatkowy mikrofon typu „gęsia szyja”
- Możliwość zasilania z wykorzystaniem standardu PoE IEEE 802.3 af

Wymagania dotyczące interkomów naściennych:

- Stacje Interkomowe w wersji IP. Funkcje diagnostyczne oraz sprawdzanie ciągłości lini; 3 wejścia bezpotencjałowe i 2 wyjścia przekaźnikowe dla sygnałów zewnętrznych, wielofunkcyjne LED; audio monitoring.
- Interkomy z wbudowaną kolorową kamerą wideo (z regulacją balansu bieli i wbudowanym ogrzewaczem. Możliwość używania jako kamery sieci IP (format wideo M-JPEG z maksymalną rozdzielczością 640 x 480 pixeli) lub też jako kamery analogowej do systemów koloru PAL czy też NTSC. Regulowany kąt widzenia do 30 stopni w pionie i poziomie)
- Podświetlane przyciski przywołania oraz miejsce na etykiety
- Stopień ochrony IP 65
- Konstrukcja poliwęglanowa
- Moduły rozszerzeń na potrzeby dodatkowych funkcji
- Mikrofon elektrytowy dookólny;
- Wzmacniacz 2,5 W klasy „D“; 2 głośniki 8 ohm.
- Zasilanie PoE lub 22 – 24 V AC / 20 – 35 V DC.

2.2.Oprogramowanie

1. System zarządzania musi być neutralny wobec producentów integrowanych systemów i urządzeń.
2. System zarządzania musi posiadać Aprobatę Techniczną, Certyfikat Zgodności i Świadectwo dopuszczenia do stosowania w ochronie przeciwpożarowej wydane przez CNBOP, w ramach której system zarządzania budynkiem realizuje współdziałanie następujących urządzeń i systemów ochrony przeciwpożarowej budynku :

a) Centrale wykrywania i sygnalizacji pożaru
b) Dźwiękowe systemy ostrzegawcze
c) Przeciwpożarowe klapy odcinające, klapy odcinające wentylacji pożarowej oraz inne elementy systemów wentylacji pożarowej (np. wentylatory oddymiające);
d) Systemy wentylacji grawitacyjnej (klapy i okna oddymiające)
e) Systemy oświetlenia awaryjnego;

f) Elementy oddzieleń pożarowych (drzwi, kurtyny, bramy);
g) Urządzenia i systemy stałych urządzeń gaśniczych;
h) Inne systemy, instalacje i urządzenia wykorzystywane lub sterowane w czasie stanu alarmu pożarowego (np. dźwigi pożarowe, schody ruchome, przejścia objęte kontrolą dostępu, itd.)
i) System musi składać się z oprogramowania i urządzeń, dopuszczonych do stosowania w ochronie przeciwpożarowej,
j) Oprogramowanie musi mieć budowę modułową. Wymiana dowolnego modułu programowego nie może wstrzymywać pracy pozostałych funkcji
k) System musi współpracować z magistralą kart wejść i wyjść przeciwpożarowych komunikujących się między sobą za pomocą szyfrowanego protokołu (np. AES)
l) System musi umożliwiać nadzorowanie i sterowanie siłownikami za pomocą protokołu MP-Bus. System musi być certyfikowany w zakresie implementacji tego protokołu przez producenta.
m) W systemie wymagane są następujące sposoby połączeń :
n) Wyjścia przekaźnikowe różnych urządzeń i systemów do wejść systemu integracyjnego,
o) Przekaźniki systemu integracyjnego do wejść sterujących różnych urządzeń i systemów,
p) Port komunikacyjny centrali integrowanego systemu do sterownika systemu integrującego
q) Port komunikacyjny integrowanych urządzeń do sterownika będącego elementem systemu integracyjnego. Dodatkowo wymaga się aby sterowniki systemu integracyjnego mogły pracować w sieci.
r) Port komunikacyjny integrowanego systemu do portu szeregowego lub gniazda Ethernet komputera systemu integracyjnego.

3. System powinien pracować w sieci komputerowej oraz umożliwiać obsługę za pomocą przeglądarki internetowej z dowolnego miejsca w budynku,
4. Wymagana jest możliwość pomiaru wielkości fizycznych typu ciągłego (np. prąd ładowania baterii, wartość napięcia, temperatury, ciśnienia itp.) z wymaganą częstotliwością nie mniejszą niż 1 Hz. Wymagana jest możliwość generowania alarmów na podstawie przekroczenia progów alarmowych
5. Oprogramowanie musi mieć możliwość pracy w środowiskach wirtualnych
6. Zdarzenia i reakcje na zdarzenia muszą być zapamiętywane w logu działań.

7. Wymagane są rozbudowane systemy poziomów dostępu dla poszczególnych grup użytkowników z możliwością zróżnicowania uprawnień dostępu do :

a. Raportów
b. Procedur alarmowych
c. Planów sytuacyjnych
d. Ustawień ogólnych
e. Opracowywania i zamykania zdarzeń alarmowych, zamykania zdarzeń nieopracowanych,
f. Przekazywania zdarzeń do innych stacji obsługi ze zróżnicowaniem uprawnień na: brak dostępu, tylko odczyt, edycję, wprowadzanie nowych, kasowanie

8. System powinien posiadać możliwość przypisywania uprawnień dla operatorów z możliwością tworzenia indywidualnych stanowisk obsługi przypisanych do operatora bądź grupy. (+ nadawanie uprawnień indywidualnie dla każdego elementu w Systemie)
9. Wymagana jest możliwość skonfigurowania systemu z wieloma stanowiskami roboczymi,
10. Wymagana możliwość skonfigurowania automatycznego kierowania zdarzeń alarmowych na odpowiednie stanowiska robocze. Dodatkowo wymagana jest możliwość przekazania zdarzenia przez użytkownika. Wymagany jest przy tym mechanizm weryfikacji czy wybrane stanowisko jest aktywne. Przy przekazywaniu zdarzenia wyświetlane są tylko aktywne stanowiska z identyfikatorem (loginem) użytkownika.
11. Wymagana jest możliwość dowolnego ustawiania kategorii zdarzeń połączona z możliwością kierowania zdarzeń na stanowiska robocze. Wymagane jest zróżnicowanie kolorów zdarzeń poszczególnych kategorii.
12. Zdarzenia muszą być prezentowane na liścia zdarzeń w jednowierszowej postaci zwięzłej. Musi istnieć możliwość edycji postaci zwięzłej – wymagana jest możliwość wyboru wyświetlanych danych spośród : lp. czas i data, nazwa (lokalizacja), zdarzenia, stan obecny, priorytet, kategoria, status, użytkownik
13. Wymagana jest możliwość ustawienia kolejności wyświetlania zdarzeń alarmowych przynajmniej według (lp., czasu, identyfikatora czujnika, zdarzenia, priorytetu, kategorii) rosnąco lub malejąco
14. Wymagane są liczniki zdarzeń oddzielne dla zdarzeń wszystkich kategorii. Musi istnieć możliwość filtrowania widoku zdarzeń na liście (stosie) alarmów na zdarzenia

wybranej kategorii poprzez prostą operację (np. kliknięcie)

15. Z widoku, w którym prezentowane są tylko zdarzenia wybranej kategorii (widok filtrowany) system MUSI powracać automatycznie do widoku zdarzeń wszystkich kategorii (widok nie filtrowany) po upływie zadanego czasu
16. Wymagana jest możliwość korelacji zdarzeń i generowania zdarzenia dodatkowego
17. Wymagana jest możliwość wykonywania backupu online oraz backupu przyrostowego. Możliwość backupu bazy danych. Możliwość odtworzenia systemu z backupu
18. Wymagana jest sygnalizacja przerwy komunikacji z każdym integrowanym systemem poprzez wyświetlenie odpowiedniego komunikatu alarmowego
19. Wymagane jest, że system zarządzania elektronicznymi systemami zabezpieczeń musi automatycznie powrócić do stanu pracy. Niezbędne składniki oprogramowania (moduły) muszą być uruchamiane automatycznie (np. usługi systemu operacyjnego).
20. Powinien umożliwiać wizualizację i sterowanie Systemem Sygnalizacji Pożaru oraz mieć możliwość sterownia wszystkimi urządzeniami pożarowymi indywidualnie oraz strefowo (zatrzymanie scenariusza na wypadek wystąpienia pożaru w danej strefie i uruchomienia w (dla) innej)
21. Powinien posiadać plany w formacie wektorowym z możliwością skalowania obrazu dla całego obszaru jak i poszczególnych budynków, stref.
22. Czujniki na planie powinny być wyświetlane warstwowo dla poszczególnych systemów
23. z możliwością wygaszania warstw i zdefiniowanych widoków (wycinków) na wypadek zdarzenia z danego systemu.
24. System powinien posiadać możliwość tworzenia raportów dziennych, miesięcznych, kwartalnych ze sprawności integrowanych systemów.
25. System powinien posiadać możliwość wykonywania okresowych testów instalacji pożarowej.
26. System powinien posiadać możliwość tworzenia indywidualnych procedur działania na wypadek zdarzenia w budynku z możliwością rozgałęzienia procedur na kolejne etapy
27. w zależność od działań podjętych przez operatora.
28. System powinien posiadać możliwość załączania dowolnych dokumentów takich jak karty katalogowe, instrukcje, przypisanych do konkretnych procedur działania, czujników lub urządzeń,
29. System powinien mieć możliwość podłączenia dowolnego za pomocą protokołu

komunikacyjnego.

30. System powinien umożliwić podłączanie dowolnych urządzeń komunikujących się za pomocą styku (sterowanie i nadzorowanie – w tym urządzenia ochrony przeciwpożarowej)
31. System powinien mieć możliwość tworzenia indywidualnych stanowisk obsługi dla poszczególnych budynków jak i możliwość nadzorowania wszystkich budynków z jednej stacji operatorskiej.
32. Należy zapewnić bezpieczne połączenie z serwerem za pomocą SSL,
33. System musi umożliwiać filtrowanie aktywnych alarmów dla dowolnego zdarzenia,
34. System musi pracować w architekturze zorientowanej na usługi (ang. SOA)
35. Wymagany jest mechanizm automatycznego wykonywania kopii zapasowych zgodnie z harmonogramem, na żądanie i z podziałem na kopiowane fragmenty systemu takie jak baza danych, logi, usługi, pliki konfiguracyjne, dokumentacje, instrukcje, zagnieżdżone elementu.
36. System musi zapewnić możliwość implementacji instrukcji bezpieczeństwa pożarowego,
37. System zarządzania elektronicznymi systemami zabezpieczeń musi posiadać moduł wprowadzania adresów i kontaktów - baza serwisantów, pojazdów itp.
38. Interfejs systemu ma mieć możliwość obsługi w języku polskim, niemieckim, angielskim

2.3.Prace remontowo adaptacyjne.

Należy opracować dokumentację remontu – adaptacji (projekt budowlany) pomieszczeń na 2 piętrze PSP na potrzeby Centrum.

Pomieszczenia biurowe należy przystosować do pełnienia funkcji całodobowego monitoringu budynków i terenów Zarządu Morskiego Portu Gdynia S.A. za pomocą zintegrowanego elektronicznicznego systemu zabezpieczeń.

W tym celu należy wydzielić pomieszczenie techniczne z jednego z pokoi biurowych na cele serwerowni oraz jadalni dla personelu.

- pow. użytkowa - 38,28m2,
- kubatura – 95,68 m3,
- wysokość pomieszczeń: - 2,5m.
- wysokość budynku: - ~10m.

Infrastruktura niezbędna do użytkowania pomieszczeń to istniejące w budynku:

- instalacje elektro-energetyczne,
- instalacje alarmowe,
- instalacja wodociągowa,
- instalacja kanalizacji sanitarnej,
- instalacja grzewcza,
- instalacja teletechniczna.
- instalacja wentylacji grawitacyjnej.

Projektowane pomieszczenia należy niezbędnie wyposażyć w klimatyzację, a w szczególności pokój 24h dozoru oraz nowe pomieszczenie serwerowni. Agregaty chłodnicze należy umieścić na dachu. Pozostałe instalacje, a w szczególności instalacje elektryczne i teletechniczne należy dostosować do potrzeb i norm. Należy również pomieszczenia wyposażyć w odpowiednie oświetlenie LED spełniające wymagania ergonomii i BHP.

Ewakuacja z pomieszczeń biurowych na 2 piętrze prowadzi poprzez korytarz i istniejącą klatkę schodową bezpośrednio na zewnątrz budynku.

Na poziomie 2 piętra znajduje się zespół sanitarny spełniający potrzeby higieniczno - sanitarne dla osób przebywających na tej kondygnacji.

Na potrzeby Centrum należy wykorzystać istniejącą instalację zasilania gwarantowanego, którą należy uzupełnić o stacjonarny agregat prądotwórczy o mocy 15 – 20 kW. Dla zapewnienia podtrzymania pracy urządzeń teleinformatycznych, przez czas niezbędny dla uruchomienia agregatu,

w szafie serwerowej zostanie zastosowany UPS.

Wejście do Centrum oraz Serwerowni należy wyposażyć w dwustronną Kontrolę Dostępu a Serwerownię w system alarmowy. Przejścia kontroli dostępu zostaną zintegrowane z istniejącym systemem ZMPG SA poprzez sieć teleinformatyczną ZMPG SA.

Do łączności bezpośredniej pracowników odpowiedzialnych za bezpieczeństwo przewidziano sieciowy system interkomowy. Interkomy połączą pracowników Centrum Monitoringu, Dyspozytora Portu, Posterunek alarmowy PSP oraz wejście do Centrum.

Tabela 7 Zestawienie urządzeń i materiałów

ZESTAWIENIE MATERIAŁÓW I URZĄDZEŃ			
Centrum Zarządzania Elektronicznymi Systemami Zabezpieczeń			
lp	**Opis**	**Model**	**szt**
1	Serwer główny systemu GEMOS	PowerEdge R530 Server :	1
2	Serwer redundanty systemu GEMOS	PowerEdge R530 Server :	1
3	Stacja operatorska GEMOS	Dell Precision Tower 3420 XCTO	5
4	Monitor do stacji klienckiej 23,8"	MONITOR DO PRACY 24/7 PD240WHV 24" DVI HDMI	7
5	Konwertery do wyniesionej klawiatury, myszki, monitora w Centrum	KVM	2
6	Stacja do obsługi monitorów Video	Dell Precision Tower 3420 XCTO	2
7	Monitor Video 42"	TVM-4200	4
8	Szafa RACK	BKT	1
9	Zasilacz awaryjny RACK	PowerWalker VI 3000 RT LCD	2
10	Sterownik KD w metalowej obudowie obsługujący 2 czytniki z komunikacją z PC, interfejs TCP/IP (Wiznet)	SD-660D/MAX LAN	2
11	Czytnik kart zbliżeniowych Mifare do współpracy ze sterownikiem KD lub rejestratorem RCP Mifare Classic lub Mifare Plus (w zależności od firmware)	ASR-805M	4
12	Zasilacz 12V DC, akumulatory 2,5A 7Ah - Zasilacz 12V stabilizowany z podtrzymaniem akumulatorowym 7 Ah	PSIUNI2	2
13	Sztaba elektromagnetyczna 12V (normal open - NO)		2
14	Przycisk wyjścia awaryjnego		2
15	Zestaw alarmowy (centrala, 4 czujki PIR, moduł GSM, zasilacz buforowy z akumulatorem)	Satel Integra 32	1
16	Zestaw mebli - stół operatora, fotele		1
17	Zestaw mebli do pomieszczeń socjalnych		1
18	Wewnętrzna instalacja LAN		1

19	Klimatyzatory		2
20	Prace remontowe (elektryczne, stolarka, malarskie, budowlane, klimatyzacja)		1
21	Agregat prądotwórczy stacjonarny	15 - 20 kW	1
22	Okablowanie zasilające	OMY 3x1mm (100m)	1
23	Okablowanie magistralne/sygnałowe	YTKSY 2x2x0,5mm (100m)	2
24	Oprogramowanie integrujące	GEMOS	1

Sieć komputerowa zewnętrzna

lp	Opis	Model	szt
1	Switch Aruba 2930F 24G 4SFP	JL259A	26
2	HPE X121 1G SFP LC SX Transceiver	J4858C	10
3	HPE X121 1G SFP LC LX Transceiver	J4859C	34
4	Kabel światłowodowy	96J	5000
5	Projekt sieci		1
6	Osprzęt sieciowy (patchcordy, gniazda itp.)		1
7	Moduły komunikacyjne do monitorowanych systemów		1

System Interkomowy

lp	Opis	Model	szt
1	GE 800 SERWER CYFROWY IP z zasilaczem	C-GE800EU.C	1
2	GE800 karta abonencka dla 4 użytkowników IP, funkcjonalność B	C-G8-IP-4B	2
3	Licencja rozszerzenia z G8 - IP- 4B do G8-IP-4D	C-L8-IP-4D.C	1
4	IP stacja naścienna - plastikowa, jeden przycisk, zintegrowana kamera,	C-WS201PICM.C	1
5	Zestaw montażowy natynkowy, dla wersji plastik i modułu rozszerzeń, format - pełen wymiar	C-WSSH50P	1
6	EE900A IP master stacja nabiurkowa interkomowa, czarna z mikrofonem na gęsiej szyjce	C-EE972AS.C	3
7	Interkom Client licencja, wersja 1.x , 1 klient	C-L-ICCAA1	2
8	Interkom Client licencja, 1 moduł wideo	C-L-ICCVA	2

3. Szkolenia

Integrator elektronicznych systemów zabezpieczeń powinien być obsługiwany przez przeszkoloną obsługę. Zakres materiału do opanowania nie ogranicza się jedynie do obsługi czy administrowania integratora, ale również obsługi poszczególnych podsystemów. Poniższa tabela przedstawia podział szkoleń użytkowników.

Szkolenia

Tabela 8 Rodzaje szkoleń

L.P.	Kod	Zakres	Użytkownik	Certyfikacja
1	PZ	Podstawowe pojęcia, parametry systemów zabezpieczeń.	Operator / administrator	Nie
2	ISZU	Integrator- obsługa i zarządzanie	Operator	Tak
3	ISZA	Integrator- Zaawansowane zarządzanie i administrowanie systemem	Administrator	Tak

PZ

Podstawowe pojęcia, parametry systemów zabezpieczeń.

Czas trwania szkolenia: 1 dzień.

Osoby szkolone: Pracownicy Centrum monitoringu

Cechy szkolenia:

Szkolenie powinno być ukierunkowane na przekazanie podstawowej wiedzy z zakresu elektronicznych systemów zabezpieczeń. Należy podzielić je na dwie części. Część pierwsza obejmie podstawowe pojęcia i parametry związane z elektronicznymi systemami zabezpieczeń oraz przekazana zostanie wiedza z podstaw prawnych. Druga część szkolenia. Obejmować powinna podstawa działania systemu integrującego, współpracującego z KD CCTV SSWiN i SSP.

Po zakończeniu tego szkolenia osoby powinny posiadać podstawową wiedzę z zakresu użytkowanych systemów w kontekście integracji, ich parametrów technicznych i przepisów prawnych.

ISZU

Integrator obsługa i zarządzanie

Czas trwania: 2 dni

Osoby szkolone: Pracownicy Centrum monitoringu, administratorzy systemu

Cechy szkolenia:

Szkolenie powinno być ukierunkowane na przekazanie podstawowej wiedzy z zakresu obsługi integratora oraz poszczególnych podsystemów bezpieczeństwa. Należy przeprowadzić je w formie teoretycznej i laboratoryjnej. Przekazana teoria powinna umożliwić poruszanie się po systemie integrującym oraz, jeżeli będzie potrzeba po poszczególnych podsystemach. W części laboratoryjnej przeprowadzi się ćwiczenia utrwalające wiedzę zdobytą wcześniej.

Po zakończeniu szkolenia osoby powinny posiadać wiedzę teoretyczną i praktyczną z zakresu obsługi Integratora na poziomie Użytkownika.

Szkolenia

ISZA

Integrator, Zaawansowane zarządzanie i administrowanie systemem

Czas trwania: 3 dni

Osoby szkolone: administratorzy systemu

Cechy szkolenia:

Szkolenie powinno być ukierunkowane na przekazanie wiedzy z zakresu administrowania Integratora. Należy przeprowadzić je w formie teoretycznej i laboratoryjnej. Przekazana teoria powinna umożliwić administrowanie systemem integrującym oraz, jeżeli będzie potrzeba po poszczególnych podsystemach. W części laboratoryjnej przeprowadzi się ćwiczenia utrwalające wiedzę zdobytą wcześniej.

Po zakończeniu szkolenia osoby powinny posiadać wiedzę teoretyczną i praktyczną z zakresu obsługi Integratora na poziomie Administrator.

4. Gwarancja

Wykonawca udzieli nie mniej niż 24 miesięczną gwarancję na całość przedmiotu zamówienia na warunkach:

1. Okres obowiązywania gwarancji dla „dokumentacji projektowej" i realizacji skończy się z dniem, gdy upłynie zadeklarowany w ofercie termin udzielenia gwarancji liczony od dnia przekazania w użytkowanie Zamawiającemu ostatniego etapu realizacji;
2. Dla zakresu „dokumentacji projektowej" od dnia jej przyjęcia przez Zamawiającego aż do dnia określonego zapisem pkt.1.
3. Dla zakresu realizacji od dnia przekazania w użytkowanie Zamawiającemu aż do dnia określonego zapisem pkt. 1.
4. Wykonanie wszystkich wymogów eksploatacyjnych stawianych przez producentów w Dokumentacji Techniczno-Ruchowej, Instrukcjach, Umowach Gwarancyjnych itp. łącznie
   z dostawą i wymianą materiałów eksploatacyjnych na zasadach i w terminach określonych przez producenta przez cały okres gwarancji zadeklarowany przez Wykonawcę.

W celu utrzymania gwarancji Zamawiający musi:

1. Wykonywać okresowe przeglądy, co sześć miesięcy, który obejmować będą wykonywanie wszystkich zaleceń eksploatacyjnych przekazanych przez Wykonawcę.
2. Dokonywanie napraw gwarancyjnych stwierdzonych w trakcie przeglądów oraz zgłaszanych przez Użytkowników;
3. Usunięcie awarii wymagającej naprawy i wymiany osprzętu technicznego w czasie nie przekraczającym 14 dni licząc od daty zlecenia usunięcia awarii.

Wykonanie konserwacji znajduje się poza obszarem gwarancji.

Wykonawca zobowiązany jest do świadczenia serwisu pogwarancyjnego, na warunkach ustalonych umową i kartą gwarancyjną, gwarantujących dostępność części zapasowych dla urządzeń systemu lub ich zamienników, dla umożliwienia ciągłości bezawaryjnej pracy systemu.

5. Odbiory

Zamawiający ustala następujące rodzaje odbiorów:

- odbiór dokumentacji projektowej
- odbiór po zakończeniu realizacji przedmiotu zamówienia z przekazaniem Zamawiającemu w użytkowanie przedmiotu odbioru

W celu dokonania odbioru przedmiotu zamówienia Zamawiający powoła Komisję Odbiorową. W skład Komisji Odbiorowej wejdą:

1. Przedstawiciele Zamawiającego, w tym Inżynier Projektu
2. Przedstawiciele Wykonawcy, w tym główny projektant systemu, kierownik budowy, kierownik robót oraz kierownik kontraktu, jeżeli takiego ustanowi Wykonawca,

Sprawdzeniu i kontroli będą podlegały:

1. jakość wykonania robót i dokładność montażu,
2. prawidłowość funkcjonowania zamontowanych urządzeń i wyposażenia,
3. poprawność podłączeń, wydajność przesyłowa.
4. Prawidłowe ustawienie integratora.

Zamawiający w celu dokonania odbioru dokumentacji projektowej wymaga przedłożenia przez Wykonawcę kompletnej dokumentacji projektowej Inżynierowi Projektu do zaopiniowania.

Inżynier Projektu sprawdzi, w terminie do 14 dni kalendarzowych od daty przedłożenia przez Wykonawcę, poszczególne części dokumentacji (projekty wykonawcze, specyfikacje techniczne wykonania i odbioru robót budowlanych) i przedłoży opinię zawierającą uwagi do dokumentacji lub potwierdzenie o kompletności tej dokumentacji oraz potwierdzi jej gotowość do odbioru.

Zamawiający przekaże Wykonawcy uwagi Inżyniera Projektu zawarte w opinii i nakaże (jeśli będą ku temu przyczyny) poprawę dokumentacji projektowej w terminie 7 dni lub podejmie decyzję skierowania jej do realizacji.

Przed przystąpieniem do prac odbiorowych Wykonawca opracuje i przedstawi do akceptacji Zamawiającemu testy akceptacyjne, w oparciu o które będzie dokonywane sprawdzenie zrealizowania funkcjonalności systemu.

Odbiory

Wykonawca zobowiązany jest do pisemnego powiadomienia Zamawiającego o zakończeniu realizacji przedmiotu zamówienia oraz zgłoszenia gotowości do odbioru przedmiotu zamówienia.

1. Do pisemnego powiadomienia o gotowości do odbioru przedmiotu zamówienia Wykonawca zobowiązany jest dołączyć wymagane dokumenty odbiorowe do Zamawiającego w skład których wchodzić będą między innymi:
2. Oświadczenie kierownika budowy o zgodności wykonania obiektu z dokumentacją projektową i obowiązującymi normami,
3. Oświadczenie o doprowadzeniu do należytego stanu i porządku terenu budowy,
4. Oświadczenie o właściwym zagospodarowaniu terenów przyległych
5. Protokoły badań i sprawdzeń, pomiary i ekspertyzy,
6. Komplet dokumentacji powykonawczej ze wszystkimi uzgodnieniami i pozwoleniami w oryginale
7. Zestawienie wbudowanych materiałów wraz z dokumentami potwierdzającymi wprowadzenie do obrotu zgodnie z obowiązującymi przepisami,
8. Inne dokumenty wynikające ze specyfikacji technicznych, warunkujące odbiór i oddanie przedmiotu zamówienia do użytku.

Gotowość Wykonawcy do odbioru potwierdzi Zamawiającemu Inżynier Projektu w terminie 14 dni od złożenia do niego przez Wykonawcę dokumentów odbiorowych, po stwierdzeniu ich kompletności i poprawności.

Zamawiający, po uzyskaniu od Inżyniera Projektu potwierdzenia o gotowości Wykonawcy do odbioru, wyznaczy termin rozpoczęcia odbioru nie późniejszy niż 20 dni od otrzymania pisemnego powiadomienia o gotowości do odbioru wraz z dokumentacją odbiorową

Wykonawca dokona rozliczenia rzeczowo-finansowego robót objętych Projektem na dzień odbioru robót przez Zamawiającego od Wykonawcy wraz z przedstawieniem danych, dotyczących przekazania środka trwałego (PT i OT) z podziałem na użytkowników i przekaże je Inżynierowi Projektu w terminie 5 dni od dnia, na który zostało sporządzone.

Odbiór i przekazanie do użytkowania nastąpi protokolarnie, na podstawie protokołu spisanego przez upoważnionych przedstawicieli Wykonawcy i Zamawiającego.

Zamawiający z tytułu stwierdzonych w trakcie odbioru wad i usterek przysługują następujące uprawnienia:

Zamawiający może odmówić odbioru przedmiotu umowy, wyznaczając termin usunięcia wad i usterek. Jeżeli wady i usterki nie nadają się do usunięcia, ale nie uniemożliwiają użytkowania przedmiotu zamówienia zgodnie z przeznaczeniem, może obniżyć wynagrodzenie należne

Odbiory

Wykonawcy . Jeżeli wady i usterki uniemożliwiają użytkowanie przedmiotu zamówienia zgodnie z przeznaczeniem lub stanowią zagrożenie użytkowania, może odstąpić od umowy bez wynagrodzenia dla Wykonawcy lub żądać wykonania przedmiotu zamówienia po raz drugi lub zlecić jego wykonanie innemu podmiotowi na koszt Wykonawcy - z tego uprawnienia Zamawiający może skorzystać po bezskutecznym upływie wyznaczonego terminu usunięcia wad i usterek.

W okresie udzielonej gwarancji Wykonawca zobowiązany jest do udziału w przeprowadzanych przez Zamawiającego przeglądach oraz do usuwania stwierdzonych w trakcie tych przeglądów wad i usterek.

Potwierdzeniem wykonania przez Wykonawcę zobowiązań z tytułu udzielonej gwarancji jest odpowiedni protokół z ostatniego przeglądu w okresie gwarancji, nie później niż 30 dni kalendarzowych przed upływem okresu gwarancji, stwierdzający brak wad i usterek lub protokół z usunięcia wad i usterek stwierdzonych podczas tego przeglądu.

Przed przystąpieniem do prac odbiorowych Wykonawca opracuje i przedstawi do akceptacji Zamawiającemu testy akceptacyjne, w oparciu o które będzie dokonywane sprawdzenie zrealizowania funkcjonalności systemu.

Przed przystąpieniem do odbioru, w dniu pisemnego powiadomienia o gotowości do odbioru, Wykonawca przedstawi do akceptacji kompletną dokumentację powykonawczą wraz z protokołami pomiarów (w ilości trzech kompletów dokumentacji oraz jeden na nośniku elektronicznym).

Po odbiorze Wykonawca przekaże Zamawiającemu komplet dokumentacji oraz wszystkie Hasła i kody do systemu.

6. Uproszczony kosztorys inwestorski

Patrz Załącznik nr 6.

Spis tabel

Spis rysunków

Załączniki