PRACOWNIA PROJEKTOWA
81-314 Gdynia, ul. Pomorska 57b/19, tel.: 58 – 622 21 79, kom.:603 98 43 57, email:projektowe.uslugi@gmail.com

Inwestor

POLITECHNIKA GDAŃSKA

ul. Narutowicza 11/12, 80-233 Gdańsk

OBIEKT:	Centrum Sportu Akademickiego Politechniki Gdańskiej 80-219 Gdańsk, Al. Zwycięstwa 12, dz. ew. nr 267/4 ob.56
TEMAT OPRACOWANIA:	**PROJEKT REMONTU I PRZEBUDOWY ŚRODKOWEJ CZĘŚCI BUDYNKU CSA PG w GDAŃSKU**
JEDNOSTKA PROJEKTOWA*:*	MW Pracownia Projektowa arch. Małgorzata Wójcik 81-314 Gdynia ul. Pomorska 57b/19
STADIUM OPRACOWANIA:	**PROJEKT BUDOWLANO-WYKONAWCZY**
TYTUŁ OPRACOWANIA:	**PROJEKT SSWiN i CCTV** **TOM IV**

Biuro Branżowe:

ROD s.c.

Ul. Grunwaldzka 471, 80-309 Gdańsk

58 352 30 34 biuro@rod.gda.pl

AUTORZY OPRACOWANIA:

Tadeusz Sągolewski
upr. bud. nr. 2262/LB/74

Adam Ćwik

Iaj 2012

81-314 Gdynia, ul. Pomorska 57b/19, tel.: 58 – 622 21 79, kom.:603 98 43 57,
email:projektowe.uslugi@gmail.com

Spis treści

Spis rysunków

CZĘŚĆ OGÓLNA

1. Podstawa opracowania

- Umowa na wykonanie projektu.
- Podkłady budowlano - architektoniczne
- Obowiązujące przepisy, normy i katalogi.
- Wytyczne Inwestora.

2. Zakres opracowania

- System Sygnalizacji Włamania i Napadu (SSWiN)
- System telewizji użytkowej (CCTV)

Przedmiotem opracowania są instalacje SSWiN oraz CCTV dla potrzeby przebudowy części budynku zwanej „Łącznikiem" w budynku administracyjno-socjalnym PG CSA Politechniki Gdańskiej w Gdańsku przy ul. Aleja Zwycięstwa 12.

I. CZĘŚĆ TECHNICZNA

1. SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU.

1.1. Podstawa techniczna opracowania

- Polska Norma PN-EN 50133-2-1:2002 Systemy alarmowe. Systemy kontroli dostępu stosowane w zabezpieczeniach. Część 2-1: Wymagania dla podzespołów
- Polska Norma PN-EN 50133-7:2002 Systemy alarmowe. Systemy kontroli dostępu stosowane w zabezpieczeniach. Część 7: Zasady stosowania
- Polska Norma PN-EN 50133-1:2000 Systemy alarmowe. Systemy kontroli dostępu. Wymagania systemowe
- Polska Norma PN-93/E-08390 Systemy Alarmowe
- Polska Norma PN- IEC 60364 Instalacje elektryczne w obiektach budowlanych. Ochrona przeciwporażeniowa.
- Wymagania techniczne na okablowanie strukturalne, Ministerstwo Łączności, Warszawa 1997. Załącznik nr 23 do rozporządzenia Ministra Łączności z dn. 04.09.1997 r.
- PN-91/E-08109: Koordynacja izolacji w instalacjach niskiego napięcia z uwzględnieniem odstępów izolacyjnych powietrznych i powierzchniowych dla urządzeń,
- Dz. U. z 2005 r. Nr 196, poz. 1631 o ochronie informacji niejawnych

1.2. Charakterystyka chronionego obiektu

a) analiza architektoniczno-budowlana

Przedmiotem inwestycji jest przebudowa pomieszczeń części budynku administracyjno-socjalnego PG CSA zwana „Łącznikiem" przy Al. Zwycięstwa, w Gdańsku. Użytkownikiem lokalu oraz Inwestorem jest Politechnika Gdańska. Powierzchnia przebudowywanej części to ok. 1720 m2.

Budynek w aranżowanej części posiada 2 kondygnacje naziemne i podpiwniczenie. Przykrycie dachem płaskim.

W zakres przebudowy wchodzą m. in.:

- budowa ścian wewnętrznych,
- budowa instalacji elektrycznej, strukturalnej
- przebudowa systemu Sygnalizacji Alarmu Pożaru,
- instalacja systemów SSWiN, KD oraz CCTV.
- Instalacja wentylacji, klimatyzacji

Lokal jest już wyposażony w pełną stolarkę okienną. Nie przewiduje się szyb przeciwwłamaniowych. Ścianki wewnętrzne projektowane z płyt GK, oraz bloczków gipsowych SILKA, sufity podwieszane, modułowe lub stropy właściwe. W pomieszczeniach szczególnie chronionych tj. serwerowni ścianki wykonane zostaną z

bloczków silka do pełnej wysokości (do stropu). Pomieszczenie serwerowni stanowi wydzieloną strefę pożarową.

Drzwi wejściowe do pomieszczeń jedno lub dwu skrzydłowe, rozwierane o normatywnych wymiarach. Drzwi wejściowe do „Łącznika" – nowoprojektowane dwie pary automatycznych drzwi rozsuwanych oraz trzy sztuki drzwi szklanych rozsuwanych w zabudowywanej części podcienia. Dodatkowo istniejące drzwi dwuskrzydłowe od strony wschodniej (z poziomu parteru) w pobliżu hali gimnastycznej. W ramach przebudowy od strony południowej projektuje się także drzwi zewnętrzne na poziom piwnicy.
Wszystkie wejścia objęte zostaną ochroną systemu SSWiN.

b) analiza topograficzna obiektu

Położenie budynku w ruchliwej części miasta o dużej gęstości zaludnienia. Obszar dobrze skomunikowany, w godzinach popołudniowych spodziewane utrudnienia dojazdu służb ochrony, Policji związany z wysokim natężeniem ruchu drogowego. W godzinach nocnych, kiedy jest największe prawdopodobieństwo włamania utrudnienia w ruchu nie występują. W okolicy występują inne budynki chronione całodobowo jak np. Filharmonia, pobliska stacja paliw czynna całodobowo, czy też Politechnika Gdańska.

c) analiza funkcjonalna obiektu i systemu

Lokal zabezpieczony będzie systemami SSWIN oraz CCTV. Ochronie podlegają części komunikacji ogólnej oraz wskazane przez Inwestora pomieszczenia – serwerownia, portiernia, wszystkie drzwi wejściowe do pomieszczeń na 1 piętrze (oprócz szatni). Pozostałe pomieszczenia bez ochrony.

Wejście główne do „Łącznika" – przez automatyczne drzwi rozsuwane chronione jest obustronnie (od wewnątrz i od zewnątrz) poprzez monitoring telewizji dozorowej oraz czujkę PIR powiadamiającą centralę sygnalizacji włamania o naruszeniach wejścia. Osoba uprawniona winna otworzyć drzwi zewnętrzne kluczem i natychmiast po wejściu (przeważnie w czasie 30s – dokładny czas zaprogramować w ustaleniu z użytkownikiem) wprowadzić kod dezaktywujący alarm w strefie wejścia na klawiaturze manipulatora M3. Kod może składać się z kombinacji 4 - 6 znaków dostępnych z klawiatury manipulatorów. W dalszym kroku należy dezaktywować strefę przeznaczenia dla danej osoby, co można zrealizować na tym samym manipulatorze M3 (ale też i na każdym innym). Zaproponowany podział na strefy alarmowe został przedstawiony w części rysunkowej. **Centrala alarmowa posiada bardzo elastyczne oprogramowanie, podziału stref w oparciu o posiadany system można dokonywać programowo, także po montażu bez potrzeby dokonywania nakładów materiałowych**.

Wywołanie alarmu poprzez czujkę w każdej strefie sygnalizowane jest poprzez uruchomienie sygnalizatorów optyczno-akustycznych, optycznych oraz poprzez informację telefoniczną – centrala telefoniczna informuje wybranych użytkowników (zaprogramowane nr. telefonów) o stanie alarmu.

Wszystkie obudowy należy trwale przytwierdzić do podłoża, zabezpieczyć przed mechanicznym otwarciem zgodnie z DTR producenta (śruby, zamki itp.) oraz chronić 24h linią antysabotażową – do tych potrzeb wydzielono odrębne linie, zgodnie ze schematem systemu alarmowego.

Zaleca się również podpisanie umowy z firmą świadczącą usługi ochrony na całodobowy monitoring systemu. Firma winna zainstalować własny moduł GSM i zapewnić odpowiednią reakcję na sygnał alarmu.

1.3. Analiza i ocena zagrożeń oraz sposobów i środków koniecznych do ich neutralizacji

Do podstawowych zagrożeń związanych z funkcjonowaniem projektowanego obiektu należą:

1) **Kradzież**; mało prawdopodobne;
   przeciwdziałanie: jawne kamery systemu CCTV, zabezpieczenie systemem SSWiN najbardziej strategicznych z punktu widzenia Inwestora pomieszczeń, właściwa polityka społeczno-kadrowa, oraz odpowiednie przeszkolenie pracowników.
2) **Kradzież z włamaniem**; mało prawdopodobne.
   Analizując statystyki można stwierdzić, iż najwięcej włamań do budynków dokonuje się przez wszelkiego rodzaju drzwi wejściowe lub przez okna. Również zdarzają się przypadki wejścia dachem, górnymi oknami, wywietrznikami, innymi otworami tzw. słabymi punktami obiektu. W przypadku przedmiotowego obiektu najbardziej prawdopodobne wydają się być włamania poprzez drzwi, okna lub dach (zbicie szyby; wyłamanie okna lub drzwi).
   przeciwdziałanie: system sygnalizacji włamania i napadu (SSWiN, CCTV) – czujki PIR, czujki magnetyczne, czujki zbicia szkła, rejestracja kamer.
3) **Napad (rozbój)**; mało prawdopodobne, szczególnie w okolicach aktywnego wejścia.
   przeciwdziałanie: system sygnalizacji włamania i napadu (SSWiN, CCTV) – przycisk antynapadowy, rejestracja kamer.
4) **Szantaż**; mało prawdopodobny, może dotyczyć zarówno firmy, jako instytucji, jaki i kluczowych pracowników.
   przeciwdziałanie: system sygnalizacji włamania i napadu (SSWiN, CCTV) – piloty antynapadowe (SSWIN), rejestracja przejść pod przymusem (CCTV), możliwość zaprogramowania w systemie haseł „działanie pod przymusem”
5) **Sabotaż**; b. mało prawdopodobny, działania zaplanowane ze strony pracowników.
   przeciwdziałanie: właściwa polityka społeczno-kadrowa, linie antysabotażowe, obudowy, podział na strefy, nadawanie uprawnień, weryfikacja danych z systemów – zapisy kamer, zdarzenia w SSWiN.
6) **Terroryzm kryminalny**, wg statystyk bardzo mało prawdopodobny w tego typu obiektach. Duża trudność w działaniach prewencyjnych.
   przeciwdziałanie: (SSWiN, i CCTV) – rejestracja otwarcia stref pod przymusem (CCTV), hasła w SSWiN „działanie pod przymusem”,
7) **Zagrożenia pożarowe**; prawdopodobne, pożar samoistny lub podpalenia.
   przeciwdziałanie: instalacja SAP (w ramach odrębnego projektu).

8) **Zagrożenia środowiskowe i ze strony infrastruktury technicznej**; b. mało prawdopodobne.
przeciwdziałanie: instalacja SAP

Na podstawie powyższej analizy:

- Klasyfikacja zagrożonej wartości Z3
- klasa urządzenia alarmowego C – profesjonalna, system alarmowy zapewniający poziom bezpieczeństwa SA3.

1.4. Opis ogólny systemu SSWiN

System sygnalizacji włamania i napadu oparty będzie o mikroprocesorową centralkę z własnym układem zasilania awaryjnego na 30 h czuwania oraz 0,5 h alarmowania.

System sygnalizacji włamania i napadu został zaprojektowany dla ochrony pomieszczeń i zabezpieczenia mienia, jako system bezpieczeństwa z rejestracją zdarzeń i możliwością ich dowolnego przeglądania. Ochrona pomieszczeń i stref realizowana będzie przy wykorzystaniu:

- cyfrowych czujek PIR, z kontrolą podejścia
- cyfrowych czujek PIR korytarzowych
- czujników magnetycznych (kontaktronowych) stanu drzwi,
- piloty uruchamiające alarm – dla obsługi.

Rozmieszczenie urządzeń systemu przedstawiają plany instalacyjne obiektu.

1.5. Opis i charakterystyka systemu.

W związku z przyjętym rozwiązaniem technicznym system umożliwia elastyczną konfigurację sprzętową i programową - łatwa rozbudowę oraz wprowadzanie zmian. Moduły rozszerzające, instalowane będą na głównych magistralach systemu i służyć mają do przekazywania sygnałów od poszczególnych detektorów (czujniki ruchu, czujniki stanu drzwi, przyciski alarmowe) do jednostki centralnej. Sygnały alarmowe zaprogramować celem wyróżnienia włamania, napadu, kradzieży bądź sabotażu. Oprócz funkcji i parametrów standardowych dostępny jest szeroki zakres funkcji i parametrów, których zmodyfikowanie umożliwia dostosowanie urządzenia do spełniania lokalnych wymagań danego systemu bezpieczeństwa.

System posiada rozbudowaną strukturę kodów dostępu, co pozwala na stosowanie kodów numerycznych oraz przypisywanie poszczególnym kodom tzw. stref czasowych tj. godzin ważności, terminów ważności a także tymczasowych kodów. System musi posiadać kilka poziomów autoryzacji (poziomów uprawnień). Użytkownik o poziomie autoryzacji „1" może tylko uzbrajać system (lub jego część) itd. System posiadać ma osobny poziom dostępu dla obsługi serwisowej, co pozwoli na modyfikację parametrów systemu oraz na funkcje diagnostyczne.

System dzięki przyjętej koncepcji konstrukcji będzie adresowalny tzn. można łatwo zidentyfikować każdy element systemu alarmowego oraz określić jego stan bez potrzeby stosowania dodatkowych elementów adresowych.

System posiada możliwość adresowania elementów indywidualnie i grupowo oraz wyposażony jest w układy antysabotażowe chroniące centrale, konsole, linie dozorowe oraz czujniki systemu. Wszystkie zdarzenia są rejestrowane w pamięci poszczególnej jednostki centralnej.

1.6. Charakterystyka elementów systemu

1.6.1. Charakterystyka centrali SSWiN

Centrala alarmowa w trakcie realizacji niniejszego projektu winna być istniejąca i zainstalowana w pom. portierni – (obszary chronione – pomieszczenia hali gimnastycznej), zgodnie z wcześniejszym projektem „Remontu Kapitalnego i Przebudowy Hali Gimnastycznej PG CSA". W związku z powyższym niniejszy projekt stanowi rozbudowę istn. systemu alarmowego. W jej ramach należy przenieść centralę alarmową wraz z istn. oprzewodowaniem do pomieszczenia serwerowni (bez jakichkolwiek zmian w części istniejącej). System alarmowy rozbudować w dalszej kolejności zgodnie z poniższym projektem.
Należy zapoznać się z projektem pierwotnym systemu alarmowego.

Dane centrali SSWiN:

- Oprogramowanie centrali przechowywane w pamięci nieulotnej typu FLASH, co umożliwia jego łatwą aktualizację bez demontażu centrali. Wystarczy połączyć centralę z komputerem za pośrednictwem portu RS-232 i uruchomić procedurę wymiany oprogramowania.
- Możliwość zapisywania zaprogramowanych w centrali ustawień do pamięci FLASH. Nawet w przypadku odłączenia baterii podtrzymującej pamięć RAM dane te zostaną zachowane.
- Możliwość dzielenia systemu na partycje i strefy (strefa = grupa wejść). Strefy mogą być sterowane przez użytkownika, timery, wejścia sterujące lub ich stan może zależeć od stanu innych stref. Możliwe jest czasowe ograniczanie dostępu do stref.
- Możliwość rozbudowy systemu poprzez dodanie modułów rozszerzających (zakres rozbudowy zależy od wielkości centrali). Tworzenie systemu na bazie modułów (w tym kontroler systemu bezprzewodowego firmy SATEL), umieszczonych w różnych częściach obiektu, w znacznym stopniu ogranicza ilość instalowanego okablowania.
- Możliwość zapamiętania w systemie od 16 do 240 haseł, które mogą być przeznaczone dla użytkowników lub też można przypisać im funkcje sterujące.
- Różnorodność form sterowania systemem alarmowym:
  – manipulator LCD,
  – klawiatura strefowa,
  – czytnik kart zbliżeniowych,
  – pilot 433 MHz (opcjonalnie, po zainstalowaniu dodatkowego modułu)
  – pilot 868 MHz (opcjonalnie, po podłączeniu kontrolera z oprogramowaniem w wersji 2.0 lub nowszym),
  – komputer z zainstalowanym programem,
  – wiadomość SMS (opcjonalnie, po podłączeniu modułu),

  - przeglądarka internetowa (opcjonalnie, po podłączeniu modułu),
  - telefon komórkowy z zainstalowaną aplikacją
  - palmtop (PDA lub MDA) z zainstalowaną odpowiednią aplikacją (opcjonalnie, po podłączeniu modułu)
- Realizacja funkcji kontroli dostępu przy pomocy klawiatur strefowych, zamków szyfrowych oraz czytników kart zbliżeniowych lub pastylek DALLAS. Kontrola stanu drzwi przez moduły nie zmniejsza ilości wejść dozorowych centrali.
- Możliwość definiowania nazw użytkowników i większości elementów systemu (stref, wejść, wyjść, modułów), dzięki którym ułatwione jest sterowanie i kontrola systemu oraz przeglądanie pamięci zdarzeń.
- Monitoring realizowany do dwóch stacji monitorujących (cztery numery telefonów) przy pomocy:
  - linii telefonicznej,
  - kanału głosowego GSM (opcjonalnie, po podłączeniu modułu GSM),
  - GPRS (opcjonalnie, po podłączeniu modułu),
  - wiadomości SMS (opcjonalnie, po podłączeniu modułu),
  - sieci Ethernet i protokołu TCP/IP (opcjonalnie, po podłączeniu modułu).
- Centrala umożliwia monitoring w kilkunastu formatach, w tym Contact ID oraz SIA.
- Powiadamianie telefoniczne o alarmach przy pomocy komunikatów głosowych lub na pager komunikatami tekstowymi. Odebranie komunikatu głosowego można potwierdzić hasłem podanym z klawiatury telefonu (DTMF).
- Odpowiadanie na telefon – funkcja umożliwiająca sprawdzenie stanu wszystkich stref centrali oraz sterowanie stanem wyjść. Realizowana jest ona po zidentyfikowaniu użytkownika (każdemu użytkownikowi można przydzielić specjalne hasło „telefoniczne”).
- Rozbudowana funkcja bieżącego wydruku zdarzeń, umożliwiająca selekcję zdarzeń. Opisy zdarzeń są zgodne ze standardem Contact ID. Oprócz tego nazwy wejść, modułów i użytkowników drukowane są tak, jak je zdefiniowano w systemie.
- Dodatkowa funkcja portu RS-232 centrali – sterowanie zewnętrznym modemem analogowym, modemem ISDN, modułem GSM, modułem ISDN oraz modułem ethernetowym – umożliwia nawiązywanie łączności z komputerem serwisu. Programowanie zdalne przez sieć telefoniczną lub Ethernet i obsługa serwisowa są w takim przypadku tak samo szybkie, jak przy programowaniu bezpośrednio z komputera przez port RS-232.
- Możliwe sterowanie w oparciu o czas, dzięki timerom uwzględniającym tygodniowy rytm pracy oraz definiowane okresy wyjątków. Dodatkowo każda strefa ma swój timer (dzienny lub tygodniowy) programowany przez uprawnionego do tej funkcji użytkownika, zapewniający automatyczne uzbrajanie i rozbrajanie.
- Ułatwione realizowanie niestandardowych funkcji sterowania dzięki możliwości realizowania złożonych operacji logicznych na wyjściach.
- Pojemna pamięć zdarzeń, w której oprócz zdarzeń monitorowanych zapamiętywane są też inne zdarzenia (dostęp użytkownika, użyte funkcje i inne).
- Oprogramowanie central alarmowych z serii umożliwia obsługę wszystkich przychodzących zdarzeń bez potrzeby indywidualnego przyznawania priorytetu poszczególnym sygnałom.

- Hierarchia wyświetlania informacji o stanie wejść (np. w manipulatorze LCD) jest następująca (od najwyższego do najniższego priorytetu): blokada, awaria, alarm sabotażowy, alarm włamaniowy, sabotaż, naruszenie, pamięć alarmu sabotażowego, pamięć alarmu włamaniowego.

1.6.2. Czujki magnetyczne

Czujki magnetyczne posiadają certyfikat klasy „C".

Czujkę magnetyczną montować na górnej, poziomej części ościeżnicy drzwiowej w odległości 20 cm od strony uchwytu do otwierania drzwi lub okna wewnątrz strefy chronionej, a magnesy na skrzydle naprzeciwko czujki magnetycznej.

Czujki magnetyczne cechują się wyjątkową wytrzymałością i niezawodną konstrukcją. Styki, pokryte rodem i zamknięte szczelnie w atmosferze tlenku azotu, mają średnią żywotność 10 mln cykli. Tak wykonany element umieszczony jest w poliuretanowej osłonie gwarantującej elastyczne i pewne zawieszenie. Całość umieszczona w aluminiowej obudowie, kabel doprowadzony w pancerzu gwarantującym wysoką odporność mechaniczną.

Podstawowe parametry techniczne:

Typ czujki NC	
Maksymalny zasięg zadziałania kontaktronu	18-20mm
Maksymalne napięcie przełączalne kontaktronu	160V
Maksymalny prąd przełączalny	250mA
Maksymalny prąd ciągły (nie przełączalny)	1,5A
Maksymalna moc przełączalna	5VA
Oporność przejściowa	130mΩ
Materiał stykowy	Ru (Ruten)
Wymiary czujki:	
- obudowa kontaktronu	58,5x16,5x15,5mm
- obudowa magnesu	58,5x15x8,5mm
- grubość podkładki pod kontaktron	3,3mm
- grubość podkładki pod magnes	3mm
Masa	22g

1.6.3. Czujki PIR

Czujka ruchu dedykowana do pracy w systemach sygnalizacji włamania i napadu. Układ optyczny czujki działa w oparciu o wysokiej jakości lustro segmentowe, które zapewnia jednakowa czułość w całym obserwowanym obszarze oraz eliminuje tzw. martwa strefę. Użycie precyzyjnego toru optycznego i zaawansowanego procesora sygnałowego w celu zapewnienia wysokiej czułości oraz odporności na fałszywe alarmy. Zaawansowany mechanizm cyfrowej kompensacji temperatury umożliwia prace w szerokim zakresie temperatur.

Dodatkowe atuty czujki to pamięć alarmów oraz możliwość zdalnego włączania i wyłączania diody LED.

Podstawowe parametry techniczne:

Napięcie zasilania	12 V DC ±15%
Pobór prądu w stanie gotowości	12 mA
Maksymalny pobór prądu	12 mA
Dopuszczalne obciążenie styków przekaźnika (rezystancyjne)	40 mA / 16 V DC
Wykrywalna prędkość ruchu	0,3...3 m/s
Czas sygnalizacji naruszenia	2 s
Zakres temperatur pracy	-10...+55 °C
Wymiary	57 x 123 x 42 mm
Wysokość montażu	2,1...3 m – zalecana 2,2

1.6.4. Czujka PIR dualna

Dualne czujki ruchu wykorzystujące tor detekcji PIR oraz mikrofalowy idealnie nadają się do wykrywania ruchu w pomieszczeniach, w których występują trudne warunki środowiskowe takie jak np.: gwałtowne skoki temperatury czy przeciągi. Dzięki niezależnej analizie różnych zjawisk fizycznych, są one niewrażliwe na typowe zaburzenia gwarantując niezawodną pracę i skuteczną ochronę.

Napięcie zasilania	12 V DC ±15%
Średni pobór prądu	24 mA ±10%
Częstotliwość pracy głowicy mikrofalowej	10,525 GHz
Dopuszczalne obciążenie styków przekaźnika (rezystancyjne)	40 mA / 16 V DC
Czas sygnalizacji alarmu	2 s
Zasięg czujnika PIR ze standardową soczewką	15 m
Zasięg czujnika MW	od 3 do 20 m
Wykrywalna prędkość ruchu	0,3...3 m/s
Klasa środowiskowa	II
Zakres temperatur pracy	-30°C...+55°C
Wymiary obudowy	63 x 136 x 49 mm
Zalecana wysokość montażu 2,4 m	

1.6.5. Czujka PIR korytarzowa

Czujki winny charakteryzować się wysoką odpornością na fałszywe alarmy, wywoływane przez szybkie zmiany temperatur, powodowane poruszającymi się zasłonami oraz małymi zwierzętami. Czujki są wyposażone w soczewki sferyczne, które dzięki dokładnemu ogniskowaniu umożliwiają pełne wykorzystanie technologii quadu logicznego. Zaawansowane przetwarzanie sygnału pozwala na precyzyjną detekcję nawet w trudnych warunkach otoczenia.

Podstawowe parametry techniczne:

Napięcie zasilania	9,5-16 V DC
Maksymalny pobór prądu	11 mA
Wykrywalna prędkość ruchu	0,3...1,5 m/s
Czas sygnalizacji naruszenia	2,5 s
Zakres temperatur pracy	-20...+50 °C

Wymiary	97 x 62 x 44 mm
Zasięg	25m
Wysokość montażu	1,5…2,4 m – zalecana

2,4

1.6.6. Radiolinie

Radiolinie służące do przełączenia systemu w tryb alarmu należy instalować w miejscach pokazanych w części rysunkowej pod stropem. Do każdej radiolinii należy zaprogramować zestaw 4 pilotów (każdy z 4 pilotów współpracuje z każdą z 3 radiolinii równorzędnie) i przekazać Inwestorowi. Sposób alarmowania (cichy, głośny) można ustawić w sposób programowy.

Podstawowe parametry techniczne:

klasa C
rodzaj modułu odbiorczego superheterodyna
czułość -115 dBm
częstotliwość 433,92 MHz
transmisja radiowa kod zmienny
pojemność pamięci 113
Napięcie zasilania:
- znamionowe 12 V DC
- maksymalne 10-15 V DC
Pobór prądu:
- spoczynkowy 17 mA
- maksymalny 40 mA
Obciążalność:
- wyjście przekaźnikowe 1A/ 30 V DC
- wyjście tranzystorowe 0,5A/ 12 V DC
- wyjście sabotażu 50mA/ 12 V DC
ilość przekaźników 1
tryb pracy przekaźnika mono lub bistabilny
zakres czasu trybu mono ~1s-4min20s
temperaturowy zakres pracy (° C) od -20 do +40 ° C
gniazdo antenowe BNC 50 Ohm
zasięgi pracy (m)* 200 – 1000
* zasięgi w zależności od typu nadajnika

1.7. Podział na strefy dozorowe

System sygnalizacji włamania i napadu proponuje się podzielić w „Łączniku” na 6 strefy dozorowych (ograniczenie systemu to 32 strefy):

- Komunikacja ogólna
- Serwerownia
- Portiernia
- Pom. dyrektora i sekretariat

- Sala konferencyjna na 1p
- Pomieszczenia 1p

Centrala alarmowa posiada elastyczne oprogramowanie. Podziału stref w oparciu o posiadany system można dokonywać programowo, także po montażu bez potrzeby dokonywania nakładów materiałowych. Ograniczenie stanowi ilość stref w systemie SSWiN, która nie może przekroczyć 32.

Numerację stref należy rozpocząć od nr. 3 – strefy 1 i 2 występują w poprzednim opracowaniu „Remontu Kapitalnego i Przebudowy Hali Gimnastycznej PG CSA"

1.8. Zasilanie instalacji

1.8.1. Zasilanie podstawowe.

Centralę oraz ekspandery wejść należy zasilić napięciem sieciowym 230 V z rozdzielni RT poprzez wydzielony i oznaczony obwód elektryczny. Linię zasilającą należy zabezpieczyć oddzielnym bezpiecznikiem bez stosowania gniazd i wtyków instalacyjnych. Połączenie kablowe wykonać jako nierozłączne. Stosować odpowiednie zasady ochrony przeciwporażeniowej. Każdy z zasilaczy należy zabezpieczyć osobnym zabezpieczeniem.

1.8.2. Zasilanie awaryjne.

Centrala włamaniowa winna być wyposażona w zasilanie awaryjne umożliwiające pracę systemu przez 30 godzin w trybie czuwania oraz 0,5 godziny w trybie alarmowania. Zasilanie to jest realizowane poprzez akumulatory o odpowiednio dobranych pojemnościach i podłączone do centrali alarmowej monitorującej w sposób ciągły stan naładowania akumulatora.

Ze względu na przeprowadzone obliczenia, dotyczące czasów podtrzymania nie można dowolnie zmieniać konfiguracji sprzętowej – nr. linii oraz osprzętu.

1.8.3. Bilans mocy.

Ekspandery 1 i 2 zaprojektowane w ramach odrębnego opracowania „Remontu Kapitalnego i Przebudowy Hali Gimnastycznej PG CSA" zasilane są z odrębnego zasilacza.
W niniejszym projekcie przewiduje się montaż dodatkowych 7 ekspanderów (nr. 3-9), z czego ekspandery (nr. 3 i 6) zostaną wyposażone we własne zasilacze o wydajności prądowej min. 1,2A. Z zasilacza ekspandera nr 3 należy zasilić odpowiednio ekspandery 3, 4, 5, a z zasilacza ekspandera 6 odpowiednio ekspandery 6, 7, 8, 9 – zgodnie ze schematem strukturalnym.

Tabela 1. Centrala alarmowa wraz z wyposażeniem.

Stan czuwania	typ urządzenia	jedn.pobór prądu	ilość urządzeń	całkowity pobór prądu **Icz**
		mA	szt	mA
Centrala alarmowa		149	1	149,00
Manipulator LCD		60	3	180,00
Czujka PIR dualna		22	1	22,00
Czujka PIR		12	1	12,00
Ekspander wejść		zasilanie własne	9	0,00
Czujka kontaktronowa		5	4	20,00
tmp		5	3	15,00
czas czuwania **t1**	**30 h**		**suma**	**398,00**
Czas doładowania akumulatora wg PN-EN 50131-1, PN-EN 50131-6 Tlad=	**24 h**			
Stan alarmowania	typ urządzenia	jedn.pobór prądu	ilość urządzeń	całkowity pobór prądu **Ia**
		mA	szt	mA
Centrala alarmowa		337	1	337,00
Manipulator LCD		137	3	411,00
Czujka PIR dualna		29	1	29,00
Czujka PIR		12	1	12,00
Ekspander wejść		zasilacz własne	9	0,00
Czujka kontaktronowa		5	4	20,00
tmp		3	5	15,00
czas alarmowania **t2**	**0,5 h**		**suma**	**809,00**
Qmin =1,25* (Icz *t1 + Ia *t2)				
akumulator	**15,4** Ah			
należy zastosować akumulator(y)	**17**			

Tabela 2 Ekspandery EXP 3-5.

Stan czuwania	typ urządzenia	jedn. pobór prądu czuwanie	jedn. pobór prądu alarmowanie	ilość urządzeń	całkowity pobór prądu **Icz**	całkowity pobór prądu **Ia**
		mA	mA	szt	mA	mA
Ekspander wejść 3		39	91	1	39,00	91,00
Czujka PIR		12	12	3	36,00	36,00
radiolinia		17	40	1	17,00	40,00
radiolinia TEMP		5	5	1	5,00	5,00
kontaktron		5	5	1	5,00	5,00
					102,00	177,00
Ekspander wejść 4		39	91	1	39,00	91,00
Czujka PIR		12	12	5	60,00	60,00
radiolinia		17	40	1	17,00	40,00
radiolinia TEMP		5	5	1	5,00	5,00
Czujka PIR korytarzowa		22	29	1	22,00	29,00
					143,00	225,00
Ekspander wejść 5		39	91	1	39,00	91,00
Czujka PIR		12	12	2	24,00	24,00
radiolinia		17	40	1	17,00	40,00
radiolinia TEMP		5	5	1	5,00	5,00
kontaktron		5	5	1	5,00	5,00
					90,00	165,00
				suma	335,00	567,00
czas czuwania **t1**	**30 h**		czas alarmowania **t2**		**0,5 h**	
Czas doładowania akumulatora wg PN-EN 50131-1, PN-EN 50131-6 Tlad=	**24 h**					
Qmin =1,25* (Icz *t1 + Ia *t2)						
akumulator	**12,9** Ah					
należy zastosować akumulator(y)	**17** Ah					

Tabela 3 Ekspander EXP 6-9.

Stan czuwania	typ urządzenia	jedn. pobór prądu czuwanie	jedn. pobór prądu alarmowanie	ilość urządzeń	całkowity pobór prądu **Icz**	całkowity pobór prądu **Ia**
		mA	mA	szt	mA	mA
Ekspander wejść 6		39	91	1	39,00	91,00
Czujka PIR korytarzowa		22	29	1	22,00	29,00
Czujka dualna		22	29	3	66,00	87,00
kontaktron		5	5	4	20,00	20,00
					147,00	227,00
Ekspander wejść 7		39	91	1	39,00	91,00
kontaktron		5	5	6	30,00	30,00
radiolinia		17	40	1	17,00	40,00
radiolinia TEMP		5	5	1	5,00	5,00
					91,00	166,00
Ekspander wejść 8		39	91	1	39,00	91,00
Czujka PIR korytarzowa		22	29	2	44,00	58,00
czujka PIR		12	12	1	12,00	12,00
kontaktron		5	5	5	25,00	25,00
					120,00	186,00
Ekspander wejść 9		39	91	1	39,00	91,00
kontaktron		5	5	1	5,00	5,00
czujka PIR		12	12	1	12,00	12,00
					56,00	108,00
				suma	414,00	687,00
czas czuwania **t1**	**30 h**		czas alarmowania **t2**		**0,5 h**	
Czas doładowania akumulatora wg PN-EN 50131-1, PN-EN 50131-6 Tlad=	**24 h**					
Qmin =1,25* (Icz *t1 + Ia *t2)						
akumulator	**16** Ah					
należy zastosować akumulator(y)	**17**					

1.9. Odbiory instalacji.

Wykonawca przedstawi następujące dokumenty:

- Dokumentację powykonawczą,
- Protokół ciągłości żył,
- Protokół pomiarów rezystancji izolacji,
- Protokół z testów zadziałania elementów systemu SSWiN - Alarm (pobudzenie 100% elementów), uszkodzenie,
- Wydruki z prób alarmowych urządzeń automatycznych (czujka, kontaktron) i pobudzenia ręcznego urządzeń nieautomatycznych (przycisk napadowy).

1.10. Sposób prowadzenia instalacji

1. Przewody prowadzić zgodnie z trasami kablowymi zamieszczonymi w projekcie:
   - w rurkach instalacyjnych fi 22 (natynkowo pod stropami właściwymi - w przestrzeni między sufitem podwieszanym, a stropem właściwym, podtynkowo w pozostałych pomieszczeniach)
2. Nie dopuszcza się prowadzenia przewodów ze zwisem ani z wykorzystaniem uchwytów instalacyjnych innych branż np. mechanicznych
3. Dla wypustów kablowych należy zostawić zapasy przewodów min. 50 cm.
4. Kable wprowadzać bezpośrednio do urządzeń przed ich podłączeniem. Dopuszcza się stosowanie puszek pośredniczących w przypadkach niezbędnych.
5. W każdym przypadku kable wprowadzać bezpośrednio ze ściany do elementów systemu, w taki sposób, żeby urządzenia przykrywały całkowicie wypust kablowy.
6. Przed wykonaniem połączeń należy sprawdzić ciągłość przewodów przez przedzwonienie oraz zmierzyć rezystancję izolacji każdego odcinka przewodu pomiędzy żyłą przewodu i ziemią oraz pomiędzy żyłami innych przewodów. Rezystancja nie powinna być mniejsza niż 5 MΩ
7. Dołączanie przewodów należy wykonać przez przykręcanie lub zaciskanie w złączkach. Przy braku takiej możliwości dopuszcza się lutowanie w miejscach, do których zapewniony jest dostęp.

Uwagi montażowe:
Rozmieszczenie urządzeń oraz schematy blokowe pokazane są na załączonych rysunkach.

- Wszystkie elementy systemu (obudowy, przyciski, klawiatura) montować w sposób uniemożliwiający w prosty sposób oderwanie od podłoża. Typ stosowanych mocowań uzależnić od rodzaju podłoża
- Klawiatury numeryczne montować we wskazanych na projekcie miejscach na wysokości 140 cm w rzędzie z innymi urządzeniami w odległości 10 cm od sąsiedniego urządzenia
- Centrale montować we wskazanym w projekcie miejscu
- Obudowy z akumulatorami montować bezpośrednio pod obudowami zasilaczy
- Zasilacze montować w pobliżu centrali.

Wykonawca zobowiązany jest dostarczyć inwestorowi dokumentację powykonawczą systemu **(wszelkie zmiany na projekcie powinny być zaznaczone na czerwono, uzgodnione i podpisane przez projektanta)**.

2. SYSTEM TELEWIZJI DOZOROWEJ (CCTV)

2.1. Opis ogólny systemu CCTV.

System telewizji przemysłowej spełnienia trzy podstawowe zadania:

- umożliwia ochronę obiektu, zdalną kontrolę wejść, ciągów komunikacyjnych oraz miejsc szczególnie ważnych dla bezpieczeństwa i ochrony obiektu.
- zapewnia weryfikację zdarzeń i alarmów otrzymanych z innych systemów tj. włamania i napadu, ppoż, kontroli dostępu jak również kontrolę poprawności ich działania.
- zapewnia rejestrację i archiwizację zdarzeń nie wykrytych bezpośrednio przez ochronę w celu późniejszej analizy przebiegu zdarzenia lub określenie tożsamości osób biorących w nim udział.

Nadzór kamer zapewni obserwacje:

- wejścia głównego;
- korytarzy komunikacyjnych;
- wejść do pomieszczeń: Serwerowni, dyrektora oraz sekretariatu

Projektowany system ma dostarczyć środki techniczne zapobiegające niebezpieczeństwom (napad, wymuszenie, szantaż, nieuprawnione wejścia) oraz w razie ich popełnienia dostarczyć możliwie jak najwięcej materiałów dowodowych.

Dodatkowo zostaną zainstalowane kamery dla wsparcia systemu sygnalizacji włamania i napadu oraz w celu zapewnienia możliwości weryfikacji zdarzeń. Zastosowany zostanie system kamer kolorowych IP przyłączonych do cyfrowego rejestratora wizji. Dane z rejestratora można pobierać poprzez sieć LAN (miejsce przyłączenia zapewni i wskaże użytkownik). Zalogowanie po podaniu poprawnego hasła możliwe z każdego miejsca LAN. Oprogramowanie klienckie należy zainstalować w szczególności na komputerze w portierni**.** Maksymalna ilość jednocześnie zalogowanych użytkowników -10. Maksymalna prędkość transmisji – 9Mbps.

Kamery w budynku pozwolą rejestrować ruch osobowy na wejściu do budynku, rejestrację gości i osób postronnych oraz wejścia i wnętrze pomieszczeń o szczególnym znaczeniu, jak OPD czy też serwerownia.

Wszystkie kamery mają możliwość pracowania w trybie detekcji ruchu dublując dodatkowo zadania SSWiN.

2.2. Urządzenia Systemu CCTV

Jako stałe kamery podstawowe wewnętrzne zastosowano kolorowe kamery kopułkowe IP o parametrach:

2.2.1. Specyfikacja kamer zewnętrznych:

- Przetwornik 1/3" CMOS w rozdzielczości 1280 X 1024,
- Obiektyw zmiennoogniskowy f=3-9; F1,2 (szeroko), F2.1 (tele) auto-iris

- **Mechaniczny filtr IR** dla funkcji Dzień i Noc
- Wbudowany **oświetlacz IR** z zasięgiem do 15 metrów
- Kompresja w czasie rzeczywistym **H.264, MPEG-4** oraz **MJEPG** (Triple Codec)
- Jednoczesna wielostrumieniowość
- Aktywna adaptacja strumieniowania dla dynamicznej kontroli ilości klatek
- Obudowa odporna na warunki atmosferyczne **IP66**
- Detekcja manipulacji dla nieautoryzowanych zmian
- Zasilanie wbudowane zgodne z **802.3af PoE**
- Cyfrowe wejście dla zewnętrznych czujników
- Wbudowany **slot kart SD/SDHC** dla przechowywania lokalnego w kamerze
- Kąty widzenia:
  31.46°~85.7° (horyzontalnie)
  25.4°~73.16° (wertykalnie)
  39.67°~99.82° (diagonalnie)
- Korekcja IR
- Moc<10W , 12VDC, 24VAC

2.2.2. Specyfikacja kamer wewnętrznych oznaczonych jako K2, K11, K12, K13:

- 1/3" CMOS sensor o rozdzielczości 1920 x1080
- Obiektyw zmiennoogniskowy f=3-9; F1,2 (szeroko) auto-iris
- **Mechaniczny filtr IR** dla funkcji Dzień i Noc
- Wbudowane diody IR o efektywnym zasięgu do 15 metrów
- Kompresja w czasie rzeczywistym H.264, MPEG-4 oraz MJEPG (Triple Codec)
- Jednoczesna wielostrumieniowość
- Aktywna adaptacja strumieniowania dla dynamicznej kontroli ilości klatek
- Detekcja manipulacji dla nieautoryzowanych zmian
- Wbudowane zgodne 802.3af PoE
- Wbudowany slot kart SD/SDHC dla przechowywania lokalnego w kamerze
- Możliwość instalacji na suficie lub ścianie
- Wsparcie ONVIF Standard ułatwiający integrację i zwiększenie interoperacyjności
- Kąty widzenia:
  31.46°~85.7° (horyzontalnie)
  25.4°~73.16° (wertykalnie)
  39.67°~99.82° (diagonalnie)
- Korekcja IR
- Obudowa kopułkowa

2.2.3. Specyfikacja kamer wewnętrznych oznaczonych jako K1 oraz od K3 do K10

- Przetwornik 1/4" CMOS w rozdzielczości 1280 X 800,
- f=3,6, F1,8
- **Usuwalny filtr IR-cut** dla funkcji Dzień i Noc

- Wbudowany **oświetlacz IR** z zasięgiem do 15 metrów
- Kompresja w czasie rzeczywistym **H.264, MPEG-4** oraz **MJEPG** (Triple Codec)
- Jednoczesna wielostrumieniowość
- Aktywna adaptacja strumieniowania dla dynamicznej kontroli ilości klatek
- Obudowa odporna na warunki atmosferyczne **IP66**
- Detekcja manipulacji dla nieautoryzowanych zmian
- Wbudowane zgodne **802.3af PoE**
- Cyfrowe wejście dla zewnętrznych czujników
- Wbudowany **slot kart SD/SDHC** dla przechowywania lokalnego w kamerze
- Kąty widzenia: 56 st H, 41 st V, 71 st D
- Korekcja IR
- Moc<4W , 12VDC, 24VAC

2.2.4. Serwer systemowy DVR-1, klient ST1 :

Istniejące, adaptowane – serwer DVR-1 znajduje się w pom. dyrektora, klient ST-1 w pomieszczeniu portierni (należy zapoznać się z dokumentacją „System monitoringu TV lekkiej hali sportowej"). Do pomieszczenia dyrektora doprowadzony jest kabel FTPw 4x2x0,5 ze switch PoE systemu monitoringu lekkiej hali sportowej. Kabel ten należy doprowadzić do pomieszczenia serwerowni (wycofać wzdłuż elewacji i wprowadzić do budynku w okolicy osi 11 – zgodnie z częścią rysunkową) i podłączyć do rutera RT-1, skąd należy wyprowadzić przewód UTP 4x2x0,5 do pomieszczenia dyrektora oraz portierni. Do routera należy także podłączyć rejestrator sali gimnastycznej oraz części basenowej przewodami UTP 4x2x0,5 – zgodnie ze schematami strukturalnymi.
Na serwerze oraz klinecie zainstalowane jest oprogramowanie systemowe do zarządzania systemem CCTV zainstalowanym w ramach projektu „System monitoringu TV lekkiej hali sportowej". Ze względu na ułatwienie obsługi oraz procedury serwisowe zaleca się wykorzystanie osprzętu tożsamego (kamer IP) do już zainstalowanego – współpracujące w ww. oprogramowaniem. Oprogramowanie umożliwia zarządzanie systemem IP do 32 kamer. Obie stacje pracują w środowisku Windows 7, 64 bit.

W celu podglądu i dokonywania nagrań z rejestratorów zlokalizowanych w pom. ratownika (część basenowa) oraz hali gimnastycznej należy na stacjach zainstalować odpowiednie oprogramowanie. Stacje DVR-1 oraz ST-1 w takim przypadku mogą współpracować jako klient z tymi rejestratorami.

2.2.5. Switch SW-2, Router RT-1 :

W pomieszczeniu serwerowni w szafie GPD należy zainstalować switch 24 portowy PoE SW-2 o poniższych parametrach do zasilania kamer IP w standardzie PoE 802.3af:

- IEEE 802.3 10BaseT
- IEEE 802.3u 100BaseTX
- IEEE 802.ab 1000BaseT
- IEEE 802.3z 1000BaseSX/LX

- IEEE 802.3x Pełny-duplex oraz kontrola przepływu
- IEEE 802.1Q VLAN
- IEEE 802.1p QoS / Class of Service, protokoły priorytetów
- IEEE802.3 Nway Auto-negotiation
- IEEE802.3af Power over Ethernet
- 10/100BaseTX ze złączami RJ-45 : 24 porty z PoE
- 10/100/1000BaseT ze złączem RJ-45 : 2
- Otwarte sloty combo SFP: 2
- Filtr ochrony portów:
- - TCP / UDP port based
  - MAC Address based
  - IP Address based
- Ustawienia VLAN:
  - Tag Based: 32
  - Port Based: 26
  - VLAN ID (Up to 4094 K)
- QoS:
  - Priority (Port Based / TOS / Diffserv / DSCP/IPv4/IPv6)
  - Class of Service Configuration
  - TCP / UDP Port Based
- Dostęp chroniony hasłem
- Włączanie / Wyłączanie PoE na portach
- Zarządzanie przez www
- Kontrola przepustowości
- Kontrola Broadcast Storm
- Port Mirroring
- Konfiguracja portów
- Programowalny timer starzenia się
- IGMP Snooping
- Trunk (do 4 portów na grupę, 2 grupy na urządzenie)
- Klient DHCP
- Quality of Service: do 2 kolejek
- Do 15.4W na port PoE
- Maksymalna moc 250W dla wszystkich portów PoE (na urządzenie)
- Styki do zasilania:
  - 1,2,3,6
- Protocol CSMA/CD

Switch podłączyć zgodnie z częścią rysunkową.

Istniejący router RT-1 o 4 portach LAN, należy wymienić na 8 portowy o analogicznych parametrach jak istniejący – Linksys WRT54G.

2.3. Projektowane rozmiary obiektów

Rozmiary obiektów na ekranie monitora powinny zapewnić odpowiednie zbliżenie obserwowanej „sceny" zapewniając spełnienie wymagań dla poszczególnych kamer w związku z ich przeznaczeniem tj. identyfikacja, rozpoznanie, detekcja, kontrola. W przedmiotowym projekcie:

B – dla potrzeb rozpoznania – obiekt powinien zajmować przynajmniej 50% wysokości ekranu monitora – Rejestracja wejścia głównego do budynku.
C – dla potrzeb detekcji intruza – obiekt powinien zajmować przynajmniej 10% wysokości ekranu monitora – w części komunikacyjnej.

2.4. Okablowanie

Okablowanie należy prowadzić:

- pod stropem właściwym - w przestrzeni między sufitem podwieszanym, a stropem właściwym - w rurach PVC montowanych do stropu lub ściany
- w innych pomieszczeniach w rurach PVC pod tynkiem
- natynkowo pod elewacją w przypadku kamer zewnętrznych

z zachowaniem wymaganych odległości pomiędzy kablami zasilającymi, a kablami sterowniczymi i transmisyjnymi.
Należy oznaczyć wszystkie kable (wizyjne, sterownicze i zasilające) w sposób trwały i czytelny na obu końcach.

Kable do kamer stosować FTP 4x2x0,5 zapewniające zarówno przesył strumienia danych oraz zasilanie urządzeń w systemie PoE.

2.5. Zasilanie.

Rejestrator DVR-1 należy zasilić z lokalnego gniazda dedykowanego dla instalacji komputerowej 230V poprzez istn. UPS o mocy 1,5 kVA. UPS zapewnia zasilanie gwarantowane w przypadku zaniku zasilania podstawowego oraz ochronę przeciwprzepięciową stacji.
Komputer należy zasilić z lokalnego gniazda dedykowanego dla instalacji komputerowej 230V.
Router RT-1 oraz switch SW-2 należy zasilić z wydzielonego obwodu z rozdzielnicy RT poprzez projektowany UPS 750VA, czas podtrzymania do 30min.

2.6. Ochrona przeciwprzepięciowa.

Kamery zewnętrzne IP, Poe należy chronić ogranicznikami przepięć do kamer zewnętrznych o parametrach:

- do strony chronionej zasięg 10m
-10/100 Mbps Ethernet
- PoE

Ograniczniki przepięć należy podłączyć z instalacją połączeń wyrównawczych..

2.7. Uwagi dla inwestora

- Przeprowadzić wizualną i funkcjonalna kontrolę wszystkich części składowych systemu CCTV. Kontrola wizualna obejmuje sprawdzenie jakości montażu, jakości funkcjonalnej, kompatybilności poszczególnych elementów systemu.
  Kontrola funkcjonalna obejmuje sprawdzenie funkcjonalnej kompatybilności poszczególnych elementów systemu. Test kontrolne należy potwierdzić protokołami,
- Przed przekazaniem systemu należy wykonać badania, które powinny wykazać, że system działa poprawnie oraz spełnia wszystkie wymagania.
- Instalator powinien zwrócić uwagę użytkownikowi na czynniki wpływające na parametry systemu, a w szczególności na wymagania dotyczące okresowej konserwacji. Wykonawca systemu powinien dostarczyć zalecenia dotyczące obsługi i konserwacji systemu. Może zostać uzgodnione, że instalator będzie wykonywał okresowo kontrolę systemu.
- Odbiór instalacji powinien odbywać się po wykonaniu całego systemu zgodnie z opracowaną dokumentacją techniczną i ewentualnymi uzgodnionymi zmianami.
- Podczas odbioru instalacji należy zamawiającemu praktycznie zademonstrować czynności obsługowe oraz sprawdzenie poprawności działania wszystkich przejść kontrolowanych. Celowe jest dokonanie w trakcie odbioru sprawdzenia skuteczności działania systemu
- Odbiór instalacji powinien być połączony z przekazaniem instalacji do eksploatacji. W odbiorze powinien brać udział konserwator systemu, który sprawował będzie nadzór nad instalacją.
- Zakład Instalacji powinien dostarczyć właścicielowi systemu pisemne instrukcje obsługi.
- Użytkownik powinien zgłaszać służbie konserwacyjnej zauważone w czasie eksploatacji nieprawidłowości w działaniu systemu.

2.8. Konserwacja

System należy okresowo poddawać konserwacji, przynajmniej raz w kwartale. Konserwacji powinna dokonać firma posiadająca niezbędne uprawnienia tj. koncesję MSWiA, licencję II stopnia pracowników wykonujących konserwację, autoryzację producenta urządzeń systemu CCTV.

Wytyczne:

- Sprawdzenie instalacji, rozmieszczenia i zamocowania całego wyposażenia i

urządzeń na podstawie dokumentacji technicznej.

- Sprawdzenie poprawności i korekta pola widzenia wszystkich kamer.
- Wyczyszczenie wszystkich szyb obudów zewnętrznych i wewnętrznych kamer
- Usunięcie kurzu ze wszystkich elementów i urządzeń systemu.
- Usunięcie kurzu i zabrudzeń z monitorów, klawiatur i innych elementów obsługowych.
- Sprawdzenie zgodności z wymaganiami wszystkich połączeń giętkich.
- Sprawdzenie zasilania całości systemu.
- Sprawdzenie archiwizacji z poszczególnych kamer.
- Sprawdzenie logów systemowych.
- Sprawdzenie poprawności oprogramowania zgodnie z dokumentacją powykonawczą.
- Sprawdzenie hasła /kodu/
- Wykonanie testu systemu wideo detekcji.
- Sprawdzenie czytelności opisów.
- Sprawdzenie połączeń masy.

3. RYSUNKI