

## Spis treści

SPIS RYSUNKÓW.....	2
1. Część ogólna.....	3
1.1 Zakres i cel opracowania.....	3
1.2 Podstawy prawno-normatywne.....	4
2. Opis Techniczny.....	5
2.4 System kontroli dostępu .....	9
2.5 Wytyczne do montażu.....	11
3. System Telewizji Dozorowej CCTV.....	12
3.1 Wstęp.....	12
3.2 Podział obiektu na strefy chronione.....	13
3.3 Opis schematu blokowego i dobór urządzeń.....	14
4. Integracja systemów.....	16
5. Konserwacja systemów.....	16
5.1 System SSWiN i SKD.....	16
5.2 System Telewizji Dozorowej CCTV.....	17
5.3 Uziemienie ochronne.....	19
6. Pomiary.....	19
7. Uwagi dla wykonawcy robót.....	20
8. Uwagi dla użytkownika.....	21

## SPIS RYSUNKÓW

Ogólny Schemat CCTV.....	T1
Schemat CCTV Kamery Zewnętrzne.....	T2
Schemat CCTV Inkubator Przedsiębiorczości.....	T3
Schemat CCTV Centrum Komputerowe.....	T4
Ogólny Schemat SKD+SSWiN.....	T5
Schemat SKD+SSWiN Inkubator Przedsiębiorczości.....	T6
Schemat SKD+SSWiN Centrum Komputerowe.....	T7
Widok Szafy Rack19”.....	T8
CCTV Zagospodarowanie Terenu.....	T9
Rzut GaraŜu int. CCTV +SKD+ SSWiN.....	T10
Rzut Parteru CCTV+SKD+SSWiN Centrum Komputerowe.....	T11
Rzut Piętra I CCTV+SKD+SSWiN Centrum Komputerowe.....	T12
Rzut Piętra II CCTV+SKD+SSWiN Centrum Komputerowe.....	T13
Rzut Dachy CCTV+SKD+SSWiN Centrum Komputerowe.....	T14
Rzut Parteru CCTV+SKD+SSWiN Inkubator Przedsiębiorczości.....	T15
Rzut Piętra I CCTV+SKD+SSWiN Inkubator Przedsiębiorczości.....	T16
Rzut Piętra II CCTV+SKD+SSWiN Inkubator Przedsiębiorczości.....	T17
Rzut Piętra III CCTV+SKD+SSWiN Inkubator Przedsiębiorczości.....	T18
Rzut Dachy CCTV+SKD+SSWiN Inkubator Przedsiębiorczości.....	T19
Karta katalogowa AXIS 221.....	Załącznik 1
Karta katalogowa AXIS 216 FD.....	Załącznik 2

# 1. Część ogólna

## 1.1 Zakres i cel opracowania

Projekt ma obejmować system:

1- SSWiN

Budynek Centrum Komputerowego

Budynek Centrum Innowacyjności

Budynek Inkubator Przedsiębiorczości

Garaż pod budynkami

2- SKD

Budynek Centrum Komputerowego

Budynek Centrum Innowacyjności

Budynek Inkubator Przedsiębiorczości

Garaż pod budynkami

3- CCTV

Budynek Centrum Komputerowego

Budynek Centrum Innowacyjności

Budynek Inkubator Przedsiębiorczości

Garaż pod budynkami

Teren wokół budynków

Teren Boiska

## – 1.2 Podstawy prawno-normatywne

- ustawa z dnia 22 sierpnia 1997r o ochronie osób i mienia ( Dz.U.Nr 114, poz. 740)
- ustawa z dnia 22 sierpnia 1999r o ochronie informacji niejawnych (Dz.U.Nr 11, poz.95) wraz  
z puzniejszymi poprawkami.
- Polska norma- Systemy Alarmowe PN-93/E-08390/14, PN-98/E-08390/4
- Podkłady budowlane.

**Projektowane systemy tworzą jedną funkcjonalną całość obejmującą cały kompleks dlatego poniższy opis swoim zakresem obejmuje całość zadania inwestycyjnego związanego z budynkami, i zagospodarowaniem terenu**

**Ze względów formalnych kompleksowa dokumentacja została podzielona na teczki, które zawierają jednakowe opisy obejmujące cały zakres pracy jednakże nie możliwe jest wykonanie częściowego zakresu prac, bez głównych serwerów zlokalizowanych w budynku Centrum Komputerowego**

## 2. Opis Techniczny

Budowę SSWiN i SKD oparto o urządzenia:

- Rozszerzony kontroler strefy – AS 1563 firmy COMPAS
- Kontroler przejścia – AS 1560 firmy COMPAS
- Subserwery AS 1561 LAN firmy COMPAS
- Server COMPAS 2026 firmy COMPAS
- Czytniki z klawiaturą KANTECH POL-2KP klasy "S" firmy KANTECH
- Czujka podczerwieni zewnętrzna HX-40AM klasa "S" firmy ARITECH
- Czujka podczerwieni PIR z antymaskingiem EV-435 AM klasa "S" firmy OPTEX
- Czujka Mikrofalowa "Alfa" klasa "S" firmy ARPOL
- Manipulator CA-5 KLED-S klasy "S" firmy SATEL
- Kontrakton DC-102 klasa "S" firmy ARITECH
- Czytnik biometryczny BioEntry Plus Mifare firmy SYSBIO
- Rygiel elektromagnetyczny 4108 – rygiel NC, 24V, 110mA firmy "KANTECH "
- Sygnalizator akustyczny wewnętrzny M21R klasa "C" firmy EBS
- Sygnalizator optyczno-akustyczny zewnętrzny AS 506 klasa "C" firmy ALDOM
- Przycisk wyjścia awaryjnego WG 2001/SG firmy "KANTECH "

Proponowany System firmy "COMPAS"

**Okablowanie:**

Dla systemu SSWiN i SKD zaprojektowano przewód YTDY 8x0,5mm

**Każdy element systemu na oddzielnej linii. ( oddzielny przewód )**

Dla połączeń pomiędzy kontrolerami wykonać przewodem UTP4x2x0,5mm kat.5e RS485

Dla połączeń pomiędzy Subserwerem a Switchami wykonać UTP4x2x0,5mm kat. 5E

Dla połączeń pomiędzy Switchami a stacjami PC wykonać UTP4x2x0,5mm kat. 5E

Dla połączeń między budynkami projektuje się wykorzystać przewód światłowodowy projektowany sieci Ethernet ( jedno włókno )

System został podzielony na 28 stref ochrony, Cały system jest klasy SA-3 z możliwością wydzielenia stref w klasie SA-4,

Do poszczególnych stref są przypisane następujące kontrolery + urządzenia wchodzące w skład systemu:

Strefa 1 – KSR19, KSR18 - ( SA-3 )

Strefa 2 - KSR17, KSR16 - ( SA-3 )

Strefa 3 – KSR15 - ( SA-3 )

Strefa 4 – KSR14, KSR13, KSR12 - ( SA-3 )

Strefa 5 – KSR11 - ( SA-4 )

Strefa 6- KSR 10 - ( SA-4 )

Strefa 7 – KSR 9, KSR 8 - ( SA-3 )

Strefa 8 – KSR 7, KSR 6 - ( SA-3 )

Strefa 9 – KSR 5, KSR 4 - ( SA-3 )

Strefa 10- KSR 3, KSR 2, KSR 1 - ( SA-3 )

- Strefa 11 – KSR 38, KSR 37 - ( SA-3 )
- Strefa 12 – KSR 36 – ( SA-3 )
- Strefa 13 – KSR 35 - ( SA-3 )
- Strefa 14 – KSR 34 - ( SA-3 )
- Strefa 15 – KSR 33, KSR 32 - ( SA-3 )
- Strefa 16 – KSR 31, KSR 30 - ( SA-3 )
- Strefa 17 – KSR 29, KSR 28 - ( SA-3 )
- Strefa 18 – KSR 27, KSR 26 - ( SA-3 )
- Strefa 19 - KSR 25, KSR 24, KSR 23 - ( SA-3 )
- Strefa 20 – KSR 22, KSR 21, KSR 20, KSR 54 ( SA-3 )
- Strefa 21 – KSR 53, KSR 52, KSR 51 - ( SA-3 )
- Strefa 22 – KSR 50, KSR 49 – ( SA-3 )
- Strefa 23 – KSR 48 - ( SA-3 )
- Strefa 24 – KSR 47 - ( SA-3 )
- Strefa 25 – KSR 46, KSR 45 - ( SA-3 )
- Strefa 26 – KSR 44 - ( SA-3 )
- Strefa 27 – KSR 43, KSR 42, KSR 41 - ( SA-3 )
- Strefa 28 – KSR 40, KSR 39 - ( SA-3 )

W celu obsługi zintegrowanego systemu bezpieczeństwa zaprojektowano stacje robocze PC wyposażone w czytniki kart magnetycznych z oprogramowaniem "InPRO".

### **Wypożyczenie stacji PC do obsługi systemu SSWiN + SKD**

- 1. Procesor Intel core quad 2,67 Mhz
- 2. Pamięci RAM 2xDDR2 2GB (PC800)
- 3. Karta graficzna komputera PC G-Force 8600GT 512Mb
- 4. Dyski twarde komputera 1xHDD MAXTOR DiamondMax22 1TB serial ATA/300 32Mb cache 7200 RPM
- 6. Karta sieciowa Linksys LNE100TX-EU PCI 10/100/1000 Mbps RJ45
- 7. Oprogramowanie do obsługi InPRO.

### **Obsługa stacji PC.**

#### **Budynek Centrum komputerowego**

Pomieszczenie stróżówki - identyfikacja osób przebywających w strefach budynków i terenu przynależnego do niego, personalizacja kart dostępu i przypisywanie uprawnień dla wszystkich stref w systemie, dostęp do archiwum, monitorowanie stanu komunikacji między elementami systemu, pełną identyfikację osób przebywających w strefach SKD, monitorowanie źródła sygnału lub sabotażu ze wskazaniem elementu czujnika, identyfikację służ SKD, Powiadomienie o stanie alarmu. Obsługa powinna zawiadomić telefonicznie odpowiednie organy po wszczęciu alarmu z systemu.

#### **- Budynek Centrum Innowacyjności**

Pomieszczenie recepcji - identyfikacja osób przebywających w strefach budynku, personalizacja kart dostępu i przypisywanie uprawnień dla stref w budynku. Powiadomienie o stanie alarmu

#### **Budynek Inkubatora Przedsiębiorczości**

Pomieszczenie recepcji - identyfikacja osób przebywających w strefach



budynku, personalizacja kart dostępu i przypisywanie uprawnień dla stref w budynku. Powiadomienie o stanie alarmu.

## **2.4 System kontroli dostępu**

System kontroli obiektu stanowi element ochrony obiektu

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa w systemie kontroli dostępu należy stosować czytniki kart zbliżeniowych z klawiaturą, oraz czytniki biometryczne.

Do pomieszczeń serwerowni proponuje się drzwi w Klasie "C" gwarantują, że dane drzwi przez 20 minut będą się bronić przed niepożądanym otwarciem lub wycięciem w nich otworu o wymiarach 40 x 40 cm. Takie drzwi muszą mieć certyfikat potwierdzający ich odporność antywłamaniową i zgodność z tą klasą – wystawia go Instytut Mechaniki Precyzyjnej.

System kontroli dostępu powinien mieć punkt emisji kart składający się stanowiska do nadawania indywidualnego numeru kart dostępu oraz ich personalizacji. ( pomieszczenie stróżówki )

### **System Kontroli Dostępu powinien uniemożliwić:**

- wejście osobom nieuprawnionym oraz wjazd pojazdów nieuprawnionych do strefy chronionej
- wejście do obiektu osobie posługującej się fałszywą lub zablokowaną kartą dostępu oraz wejście powtórne na tę samą kartę bez uprzedniego odnotowania wyjścia.

### **System Kontroli Dostępu zapewnia:**

- płynną i kontrolowaną przepustowość pracowników i interesantów

dostęp do obiektu interesantom ( gośćmiom) poprzez wydawanie im kart dostępu uprawniających do wejścia do niego.

- Wejście do obiektu w przypadku awarii czytnika kart poprzez zwolnienie zamknięcia drzwi lub innego mechanicznego urządzenia blokującego przez operatora, po uprzednim sprawdzeniu danych personalnych osoby posiadających stosowne uprawnienia.
- Monitorowanie i identyfikacje osób w poszczególnych strefach ochrony.
- Logowanie kart dostępu przez administratora w obiekcie.
- Szybkie lokalne odblokowanie przejść kontrolowanych przez system kontroli dostępu w razie pożaru, ewakuacji, alarmu lub innego zdarzenia losowego.
- Odblokowanie lokalne przejść w razie awarii systemu.
- Nawiązanie łączności pracownika lub interesanta z operatorem systemu z centru nadzoru w chwili awarii czytnika kart i potrzeby odblokowania drzwi lub innego mechanicznego urządzenia blokującego.

Alarmowe blokowanie uprawnień karty dostępu lub ich zamianę.

- Ewidencja osób, które są obsługiwane przez system.
- Rejestrowanie i wydruk w czasie rzeczywistym wszystkich zdarzeń zaistniałych w systemie z podaniem typu zdarzenia, czasu i daty jego zajścia z opóźnieniem nie dłuższym niż 60s
- lokalizacje ostatniego użycia karty przez podanie danych dotyczących danych czytnika, dnia i czasu jej użycia.
- Wykonywanie przez operatora raportów wejścia lub wyjścia z poszczególnych stref .
- Poprawną pracę sterowników w przypadku chwilowego zaniku połączenia z komputerem
- kontrole wejścia i wyjścia

- wyświetlanie i wydrukowanie listy obecności osób pracujących w obiektach oraz interesantów
- tworzenie stref czasowo-przestrzennych lub poziomów dostępu
- Przydzielanie i blokowanie oraz zmianę poziomu dostępu dla osób
- Łatwość obsługi.

**System kontroli dostępu powinien sygnalizować:**

- natychmiastowe wykrycie uszkodzenia w systemie
- sabotaż ze wskazaniem jego lokalizacji
- otwarcie przejścia kontrolowanego bez przyznania dostępu ze wskazaniem jego lokalizacji oraz wchodzenie do programu systemu kontroli dostępu przez osobę nieuprawnioną.

## ***2.5 Wytyczne do montażu***

Czujniki ruchu montować na wysokości 2,3 do 2,6m w rogach pomieszczeń

Czujniki magnetyczne montować na wysokości ok. 1,4m wewnątrz chronionych pomieszczeń

Kontrolery montować na wysokości min 2,2m od podłoża w strefach chronionych

Połączenia w kontrolerach wykonać wg. dokumentacji technicznej producenta

Połączenia elementów liniowych czujek należy wykonać wg. dokumentacji producenta

Wszystkie urządzenia muszą być objęte ochroną anty sabotażową

Czujki ruchu muszą posiadać funkcje antymaskingu

Instalacje magistrali systemowej wykonać 4 żyłowym przewodem ekranowanym

Okablowanie zasilające 230V wykonać przewodem 3 żyłowym na napięcie przebicia 750V

### **3. System Telewizji Dozorowej CCTV**

#### **3.1 Wstęp**

W projekcie kompleksu budynków biurowych na potrzeby szczecińskiego parku naukowo -technologicznego przy ul. Niemierzyńskiej w Szczecinie został zaprojektowany system monitoringu wizyjnego CCTV w technologii IP. Projektuje się Główny punkt dystrybucyjny w pomieszczeniu specjalnie wydzielonym do tego celu. GPD składa się z 1 szafy rack19" 42 U z wyposażeniem. Na terenie obiektu zaprojektowano 139 kamer IP AXIS221, w tym 24 kamer stałe zewnętrzne przystosowane do pracy w dzień i w nocy z obiektywem zmiennoogniskowy, 118 kamer stałych wewnętrznych AXIS 216FD. Celem zaprojektowanej instalacji CCTV jest umożliwienie nadzoru rejestracji oraz podglądu terenu obiektu sportowego z możliwością wykrycia intruza . Umożliwi to wykrycie niebezpiecznych zdarzeń na terenie całego obiektu . Obserwacja terenu będzie odbywać się za pomocą kamer zewnętrznych i wewnętrznych.

Rejestracja obrazu będzie odbywała się na macierzy dyskowej iSCSI umieszczonej w szafie rack19" przeznaczonej do obsługi CCTV

#### **Urządzenia wizyjnej detekcji powinny zapewnić:**

- wykrywanie osób intruzów naruszających strefą chronioną w każdych warunkach atmosferycznych

- automatyczne przełączenie na ekran monitora zobrazenia z kamery obserwującej strefę chronioną w której nastąpiło naruszenie strefy.
- Możliwość obserwacji jednocześnie ze wszystkich kamer, wyboru obrazu z określonej kamery.
- Możliwość przeglądania listy zdarzeń
- Możliwość analizy zdarzeń w czasie rzeczywistym obserwowanych stref
- Rejestracje i odtwarzanie wszystkich zdarzeń wykrytych i zaistniałych w systemie
- Ciągłą rejestrację zdarzeń w czasie wyszukiwania i przeglądania archiwalnych zapisów
- możliwość kasowania przedawnionych zapisów archiwum

#### **NIE NALEŻY KASOWAĆ ZAPISÓW Z OSTATNICH 31 DNI.**

- Ciągłą analizę obecności sygnału wizyjnego
- Ciągłą pracę systemu w czasie przejścia z zasilania podstawowego na zasilanie awaryjne
- Zajętość łącza Ethernet dla systemu ( przyjęto 20% rezerwę )  
CCTV: 100 Mb/s
- Parametry Kamer podane w załącznikach 1 i 2. ( DTR kamer )

### **3.2 Podział obiektu na strefy chronione**

Ze względu na ilość i przeznaczenie budynków projektuje się rozproszony system telewizji przemysłowej w technologii IP opartej na punktach dystrybucyjnych zlokalizowanych w budynkach całodobową ochroną SSWiN

**Monitoringiem objęto Teren wokół budynków, wejścia do budynków oraz**

**teren boiska**

Dla prawidłowej funkcjonalności system należy podzielić na strefy obserwacji. Proponuje się dla każdego piętra w budynkach oddzielną strefę obserwacji.

- Dla wszystkich stref włącznie z kamerami zewnętrznymi główna obserwacja będzie odbywała się w budynku centrum komputerowego w pomieszczeniu służby stróżówki, na 16 monitorach LCD20”, dodatkowa obserwacja będzie odbywała się na stacjach monitorujących 3 monitorowych wyposażonych w komputer PC

**3.3 Opis schematu blokowego i dobór urządzeń**

System monitoringu wizyjnego oparty na wydzielonej części sieci LAN ze strukturą opartą o punkt dystrybucyjny.

Łączna ilość zapisu z kamer przez okres 31dni – 31TB.

Minimalna przepustowość łącza dla kamer to: 80Mb/s

**Konfiguracja Punktu dystrybucyjnego**

Szafa rack19” 42U 800x600mm

Switche z zasilaniem POE

Panele krosowe RJ45

Dla szafy rack19” projektuje się 4 macierze dyskowe iSCSI w każdej 12 dysków 750Mb

W celu utrzymania zasilania awaryjnego dla kamer i punktów dystrybucyjnych w projekcie branży elektrycznej ( agregat )

**Minimalne wymagania sprzętowe stacji PC dla CCTV ( stacja 3 monitorowa)**

- Procesor Intel core quad 2,67 Mhz
- Pamięci RAM 2xDDR2 2GB (PC800)
- Karta graficzna komputera PC G-Force 8600GT 512Mb
- Dysk twardy komputera 1xHDD MAXTOR DiamondMax22 1TB serial ATA/300 32Mb cache 7200 RPM
- Karta sieciowa Linksys LNE100TX-EU PCI 10/100/1000 Mbps RJ45
- Oprogramowanie NVR ENTERPRISE

**Minimalne wymagania sprzętowe stacji PC dla CCTV ( stacja główna 16 monitorowa)**

- Procesor Intel core quad 2,67 Mhz
- Pamięci RAM 2xDDR2 2GB (PC800)
- 2x Karta graficzna komputera PC MATROX M9188
- Dysk twardy komputera 1xHDD MAXTOR DiamondMax22 1TB serial ATA/300 32Mb cache 7200 RPM
- Karta sieciowa Linksys LNE100TX-EU PCI 10/100/1000 Mbps RJ45
- Oprogramowanie do obsługi CCTV – NVR ENTERPRISE

**W systemie telewizji dozorowej CCTV zastosowano 2 rodzaje kamer:**

- kamery zewnętrzne AXIS 221 w zestawie obudowa z grzałką PoE, montaż zewnętrzny na słupach boiska sportowego – należy użyć adaptera słupowego WSFP, montowanie za pomocą opasek metalowych ślimakowych.

Zaleca się zamontowanie obiektywu PANTAX Varifocal Lens 5-50mm dla kamer zewnętrznych AXIS 221 na boisku.

- Kamera kopułkowa wewnętrzna AXIS 216FD PoE

#### **System okablowania dla monitoringu wizyjnego:**

Dla kamer montowanych wewnątrz budynków lub na budynkach przewód UTP4x2x0,5mm katy.5e

Dla kamer montowanych na zewnątrz na słupach oświetleniowych UTP4x2x0,5mm kat. 5e PE ŻEL

Dla boiska została zaprojektowana kanalizacja teletechniczna wraz ze studniami kablowymi. SK-1

120mb orurowania DVK110

2x studnia kablowa SK-1

## **4. Integracja systemów**

Zaprojektowany system SSWiN oraz SKD umożliwia integracje z innymi systemami poprzez styk RS 232

## **5. Konserwacja systemów**

### **5.1 System SSWiN i SKD**

Wykaz czynności, które należy wykonać w trakcie przeprowadzonych okresowych przeglądów konserwacyjnych



- oględziny stanu technicznego systemów
- sprawdzenie rozmieszczenia i stanu zamocowania urządzeń systemów
- sprawdzenie zgodności z wymaganiami wszystkich połączeń giętkich
- sprawdzenie stanu wszystkich zacisków śrubowych, punktów lutowniczych instalacji
- czyszczenie i odkurzanie , sprawdzenie stanu zamknięć urządzeń systemów, zasilaczy krosownic, szyfratorów pojemników na akumulatory itp.
- Sprawdzenie poprawności działania wszystkich czujek i oczyszczenie torów optycznych czujek podczerwieni i obiektywów kamer
- sprawdzenie pracy zasilaczy i pojemności źródeł zasilania awaryjnego (akumulatorów) SKD i SSWiN
- Sprawdzenie pracy urządzeń decyzyjnych systemów zgodnie z procedurą zalecaną przez producenta.
- Sprawdzenie pracy szyfratorów, klawiatur, sterowników oraz czytników systemu
- Sprawdzenie stanu każdego urządzenia akustycznego i akustyczno-optycznego
- Skanowanie powierzchni dysków dla systemu SSWiN i SKD

## **5.2 System Telewizji Dozorowej CCTV**

Po zakończeniu prac instalacyjnych i przed jej uruchomieniem wykonawca powinien dokonać następującego sprawdzenia i pomiarów instalacji:

- kontrola zastosowań urządzeń i materiałów,
- kontrola wykonywanych połączeń,
- kontrola zainstalowanych krzyżowań i wspólnych odcinków z innymi instalacjami,

- sprawdzenie instalacji ze względu na zwarcia lub przerwy, które mogły zaistnieć
- sprawdzenie rezystancji obwodów
- sprawdzenie rezystancji żył

Dla instalacji należy założyć Książkę Eksploatacji Systemu Telewizji Przemysłowej ( KESTP ), gdzie powyższe dane wykonawca powinien zamieścić przed oddaniem instalacji do użytkowania, jako pierwszy wpis.

Po dostarczeniu urządzeń i wykonaniu instalacji CCTV, wykonawca w oparciu o załączone do urządzeń indywidualne instrukcje obsługi powinien sporządzić szczegółową instrukcję obsługi systemu. Powinna zawierać indywidualną dokumentację poszczególnych urządzeń wraz z warunkami gwarancji.

Powinna też być dostarczona Książkę Eksploatacji Systemu Telewizji Przemysłowej, w której to wpisane będą wszelkie uwagi o systemie, wykonane przeglądy, oraz ew. Awarie i naprawy.

Ze względu na możliwości systemu i stopień jego skomplikowania, przed oddaniem do użytkowania, wykonawca powinien przeprowadzić szkolenie dla użytkowników systemu CCTV. Po szkoleniu powinna zostać wyznaczona osoba odpowiedzialna za czuwanie nad bieżącą eksploatacją systemu telewizji przemysłowej.

W celu zagwarantowania bezawaryjnej eksploatacji należy raz w miesiącu dokonać sprawdzenia funkcjonalności systemu i wykonać bieżący przegląd techniczny.

W okresie 1 roku od daty przekazania systemu do użytkowania obowiązek ten powinien spoczywać na wykonawcy w ramach obsługi gwarancyjnej. Podczas przeglądu należy sprawdzić działanie całego systemu i poszczególnych jego elementów. Przegląd takowy powinien zakończyć się protokołem i odpowiednim wpisem do KESTP.

### **5.3 Uziemienie ochronne**

Szafę CCTV należy połączyć z uziomem ochronnym budynku linką miedzianą LgY 16 mm<sup>2</sup>.

Po wykonaniu połączeń z uziomem budynku wykonać pomiary, wartość uziomu nie może przekraczać 10 ohm

## **6. Pomiary**

Pomiarów należy dokonać w pełni cyfrowym przyrządem testującym firmy FLUKE DSP-4100.(urządzenie przykładowe)

Miernik przeznaczony jest do testowania połączeń miedzianych i światłowodowych w sieciach komputerowych i wszelkiego typu szybkich systemach transmisyjnych oraz analizowania ruchu sieciowego w systemach 10BASE-T i 100BASE-TX.

W stosunku do odpowiedników analogowych, DSP-4000.

Testowanie odgórne (top down)- zakłada początek testowania od najwyższej warstwy sieciowej, po czym kolejno są diagnozowane coraz niższe warstwy sieci.

Jest ona stosowana głównie w sieciach już działających, nawet współbieżnie z eksploatacją sieci. W tym sposobie testowania najpierw sprawdza się poprawność aplikacji między głównymi węzłami sieciowymi, następnie komunikację węzłów pośredniczących i dopiero na końcu poprawność poszczególnych kanałów fizycznych sieci teletransmisyjnej.

Testowanie oddolne (bottom up), testowanie sieci rozpoczyna się od warstwy najniższej, czyli sprawdzania kabli i połączeń fizycznych, i stopniowo przechodzi do diagnozowania coraz wyższych warstw. Testowanie oddolne stosuje się zwykle podczas uruchamiania sieci nowych, w praktyce należy użyć

naprzemiennie obydwóch sposobów diagnozowania sieci teleinformatycznej. Sposób testowania lokalnych sieci komputerowych LAN w zasadzie nie podlega standaryzacji, lecz ma zapewnić utrzymanie ciągłości działania sieci z określoną przepływnością (od 4 Mb/s do 100 Mb/s, w sieciach Ethernetu), nieprzerwany dostęp do zasobów lokalnych, wysoką jakość transmisji (stopa błędów od  $10^{-8}$  do  $10^{-11}$ ) w zależności od wymagań - przy zachowaniu odpowiedniej efektywności (czasu reakcji) oraz bezpieczeństwa sieci (wierność i poufność informacji). Najczęściej stosowane procedury lokalizujące uszkodzenia i diagnozujące sieci komputerowe należą:

- testowanie okablowania;
- dekodowanie strumienia danych wraz z analizą pakietów i protokołów;
- testowanie połączeń między wybranymi węzłami sieci;
- statystyczna analiza trafiku sieciowego;
- analiza konfiguracji i bieżącego stanu sieci;
- testowanie funkcji i realizacja procedur samo testowania. Zgodnie z warstwową architekturą sieci można wydzielić następujące rodzaje pomiarów sieci komputerowych: pomiary parametrów fizycznych okablowania (miedzianego i światłowodowego), pomiary pasywne dokonywane wyłącznie przez obserwację i monitorowanie funkcjonowania sieci za pośrednictwem analizatorów oraz aktywne pomiary logiczne z możliwością iniekcji do sieci wybranych zestawów testowych.

## 7. Uwagi dla wykonawcy robót

Całość prac w fazie wykonawstwa wykonać zgodnie z obowiązującymi aktualnie przepisami i normami (PN, BN, BHP, P.poż.).

Wszystkie połączenia wykonać szczególnie starannie, ponieważ instalacje w obiekcie muszą odznaczać się pewnością działania i odpornością na awarie.

Wszystkie kable sieci CCTV, SSWiN oraz SKD prowadzić zgodnie z zasadami przyjętymi

w telekomunikacji. Montaż urządzeń wykonać w oparciu o instrukcje instalowania oraz dokumentację techniczno- ruchową dostarczane wraz z urządzeniami.

Przeprowadzić przeszkolenie wyznaczonych przez inwestora osób oraz dostarczyć instrukcje użytkowania i obsługi poszczególnych elementów systemów.

## **8. Uwagi dla użytkownika**

Po przekazaniu instalacji do eksploatacji należy zlecić jego stałą konserwację zapewniającą prawidłowość i pewność jej działania.

Należy wyznaczyć fachową (przeszkoloną) stałą obsługę. Instrukcje obsługi i dokumentację techniczno ruchową poszczególnych urządzeń dostarczane są przez producenta wraz z urządzeniami.