

1.	Podstawa prawna opracowania	2
2.	Obowiązujące przepisy i normy.....	2
3.	Zasilanie obiektu	2
4.	Wyłącznik główny	2
5.	Oświetlenie podstawowe	2
6.	Oświetlenie awaryjne/bezpieczeństwa	3
7.	Układanie kabli.....	3
8.	Instalacje odbiorcze gniazd	3
9.	Uwagi końcowe:	4
10.	Ochrona od porażeń prądem elektrycznym.....	4
11.	Uziom budynku	4
12.	System kontroli dostępu KD	4
13.	System monitoringu CCTV	7
14.	Instalacja teletechniczna zewnętrzna	15
15.	Obliczenia techniczne	16
16.	Uwagi końcowe.....	16

Spis rysunków

ZT

ZAGOSPODAROWANIE TERENU - IE	TOM4.3_IEx.1
------------------------------------	--------------

KUB.

RZUT BUD. SANITARIATÓW INSTALACJE ELEKTR., TT	TOM4.3_IE.1
---	-------------

SCHEMATY

SCHEMAT ZASILNIA	TOM4.3_IEx1
SCHEMAT ROZDZ. R.GL	TOM4.3_IEx2
SCHEMAT SZAFY SK4	TOM4.3_IEx3
SCHEMAT SZAFY SK6	TOM4.3_IEx4
SCHEMAT KANALIZACJI TT	TOM4.3_ITS1
SCHEMAT CCTV	TOM4.3_ITS2
SCHEMAT KD	TOM4.3_ITS3

1. Podstawa prawna opracowania

- umowa pomiędzy Inwestorem a projektantem
- koncepcja rozwiązań techniczno - technologicznych oraz ustalenia pomiędzy Inwestorem, a Projektantem
- projekty branżowe instalacji i architektury
- obowiązujące normy i przepisy
- katalogi, karty katalogowe producentów.

2. Obowiązujące przepisy i normy

- Dyrektywa z dnia 12 grudnia 2006 r. w sprawie harmonizacji ustawodawstwa państw członkowskich odnoszących się do sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia
 - Dyrektywa z dnia 15 grudnia 2004 r. w sprawie zbliżenia ustawodawstwa Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej
 - Dyrektywa z dnia 21 grudnia 1988 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich odnoszących się do wyrobów wykonawczych
 - Norma PN-EN 12464 Światło i oświetlenie. Oświetlenie miejsca pracy – część 1: Miejsca pracy we wnętrzach
 - Norma PN-EN 62305 Ochrona odgromowa obiektów wykonawczych
 - Norma wielo-arkuszowa PN-IEC 60364 Instalacje elektryczne w obiektach wykonawczych wraz z wprowadzoną Normą PN-HD 60364 Instalacje elektryczne niskiego napięcia
 - Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie
 - Rozporządzenie Ministra Infrastruktury z dnia 3 lipca 2003 r. w sprawie szczegółowego zakresu i formy projektu budowlanego
 - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2006 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów wykonawczych i terenów
 - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 czerwca 2003 r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej
 - Ustawa z dnia 10 kwietnia 1997r. Prawo Energetyczne
 - Ustawa z dnia 13 kwietnia 2007r. o kompatybilności elektromagnetycznej
 - Ustawa z dnia 16 kwietnia 2004 r. o wyrobach wykonawczych
 - Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej
 - Ustawa z dnia 7 lipca 1994r. Prawo budowlane
- Podstawa prawna opracowania, zakres
- umowa pomiędzy Inwestorem a projektantem
 - koncepcja rozwiązań techniczno - technologicznych oraz ustalenia pomiędzy Inwestorem, a Projektantem
 - projekty branżowe instalacji i architektury
 - obowiązujące normy i przepisy
 - katalogi, karty katalogowe producentów.

3. Zasilanie obiektu

Zasilanie obiektu realizowane będzie zgodnie z wydanymi warunkami technicznymi przyłączenia z sieci ENEA Operator sp. z o.o., poprzez projektowane złącze kablowo pomiarowe ZKP-1Pp posadowione przy istniejącej stacji transformatorowej, zakres przyłącza w zakresie ENEA Operator sp. z o.o..

4. Wyłącznik główny

Dla obiektu projektuje się zmontowanie przeciwpożarowego wyłącznika głównego prądu na obudowie rozdzielnic R.GŁ. Jako element wykonawczy projektuje się wyłącznik z cewką wzrostową zamontowany w obudowie zewnętrznej. Zasilanie cewki wzrostowej wyłącznika głównego projektuje się przy wykorzystaniu przełącznika faz. Do przycisków PPWP należy prowadzić przewód 5x1,5mm.

5. Oświetlenie podstawowe

Zaprojektowano oświetlenie wnętrz zgodnie z normą PN-EN 12464-1, zastosowane oprawy oświetleniowe ze źródłem światła LED, należy traktować jako przykładowe, z możliwością zamiany na inne o równoważnych parametrach tak

aby uzyskane za pomocą ich oświetlenie było zgodne z normą. Do opraw oświetleniowych należy stosować przewody YDY 3x1,5mm lub YDY 4x1,5mm w zależności od potrzeb, łączniki światła należy montować w przedziale $h=1,1 \sim 1,4m$.

Przyjęte natężenie oświetlenia dla poszczególnych pomieszczeń zgodnie z normą i przeznaczeniem:

- Hol 200lx
- Korytarz 100lx
- pom. techniczne 100lx
- pom. biurowe 500lx
- WC 200lx

Współczynnik równomierności nie może być gorszy niż 0,5 – 0,7. Szczegóły zgodnie z załączonymi obliczeniami oświetlenia.

6. Oświetlenie awaryjne/bezpieczeństwa

Oświetlenie awaryjne w budynku obliczono zgodnie z normą PN-EN-1838. Projektowane oświetlenie awaryjne ma zapewnić oświetlenie na drodze ewakuacyjnej podczas zaniku zasilania podstawowego. Zgodnie z EN 60598-2-22 oprawy oświetleniowe do oświetlenia ewakuacyjnego usytuowano w pobliżu drzwi wyjściowych oraz takich miejscach aby zwrócić uwagę na niebezpieczeństwo, w tym hydrantów, urządzeń ppoż.

W budynku przewiduje się montaż opraw oświetlenia awaryjnego opartego na technologii LED z 1 godz. układem podtrzymania zasilania – system oparty na oprawach autonomicznych.

Oświetlenie ewakuacyjne i kierunkowe zaprojektowano na klatce schodowej oraz głównych ciągach komunikacyjnych. Wymagane natężenie oświetlenia awaryjnego na drodze ewakuacyjnej musi wynosić 1,0 lx, a w przy urządzeniach ochrony ppoż. 5lx – zgodnie z PN.

W celu zasilenia inwerterów w oprawach oświetleniowych należy prowadzić dodatkową „żyłę fazowa” bezpośrednio z zabezpieczenia danego obwodu z pominięciem łączników klawiszowych itp.

Punkty świetlne awaryjnego oświetlenia ewakuacyjnego muszą posiadać certyfikat CNBOP.

7. Układanie kabli

Kable należy układać na głębokości 0,7m poza pasem drogowym, a w pasie drogowym na głębokości 1,0m, na warstwie piasku o grubości co najmniej 10cm. Kable powinny być ułożone w wykopie linia falistą z zapasem (3% długości wykopu) wystarczającym do skompensowania możliwych przesunięć gruntu. Ułożone kable należy zasypać warstwą piasku o grubości co najmniej 10 cm, a następnie warstwą gruntu rodzimego o grubości co najmniej 20 cm. Trasa kabla powinna być na całej długości oznaczona folią z tworzywa sztucznego o trwałym niebieskim kolorze. Odległość folii od kabla powinna wynosić co najmniej 30 cm, a jej szerokość być nie mniejsza niż 20 cm. Pozostałą część wykopu wypełnić gruntem rodzimym. Przy przejściu pod drogami i wjazdami kable układać na głębokości 1m w przepustach wykonanych z rur AROT typu DVK 75 w kolorze niebieskim o średnicy 75mm. Skrzyżowania i zbliżenia kabli z istniejącym uzbrojeniem podziemnym należy wykonać zgodnie z PBUE i PN. W przypadku, gdy z uzasadnionych względów odległości wymagane przez normę nie mogą być zachowane, należy zastosować rury ochronne z PCV. Kable ułożone w ziemi powinny być zaopatrzone na całej długości w trwałe oznaczniki rozmieszczone w odstępach nie większych niż 10 m oraz przy mufach i w miejscach charakterystycznych, np.: skrzyżowaniach, wejściach do rur osłonowych, na końcach kabli. Całość robót kablowych wykonać zgodnie z projektem oraz normami kablowymi PN-76/E-05125, N-SEP 004.

8. Instalacje odbiorcze gniazd

W pomieszczeniach biurowych, reprezentacyjnych, korytarzach instalację gniazd 230V wykonać przewodami - YDYp 3x2,5mm² jako wtynkowe układając przewody od gniazda do gniazda na wysokości 0,3 - 0,5m od poziomu podłogi. Zabrania się podłączania więcej niż dwóch przewodów pod zaciski pojedynczego gniazda. Stosować osprzęt instalacyjny wtynkowy IP20, w łazienkach i pomieszczeniach wilgotnych IP44. W pomieszczeniach magazynowych, łazienkach, pom. technicznych gniazda montować na wysokości 1,4m.

W pomieszczeniach technicznych, dopuszcza się wykonanie instalacji jako natynkowej w rurkach osłonowych.

Obwody gniazd zabezpieczone są wyłącznikami różnicowo-prądowymi o $\Delta I=30mA$. Obowiązkowo zachować strefę ochronną 60cm od krawędzi wanny lub natrysku w której zabrania się montowania urządzeń elektrycznych.

9. Uwagi końcowe:

1. Roboty na budowie powinny być wykonane zgodnie z PN-76/E-05125 „Elektroenergetyczne i sygnalizacyjne linie kablowe – projektowanie i budowa”.

2. Przed przystąpieniem do robót należy na 7 dni naprzód powiadomić właścicieli i użytkowników instalacji oraz urzędów o przystąpieniu do robót celem wyznaczenia z ich strony nadzoru technicznego. Należy też uwzględnić uwagi zawarte w uzgodnieniach.

4. Dla 0,4kV należy wykonać po wykonawcze pomiary geodezyjne.

5. Po zakończeniu prac teren należy doprowadzić do stanu pierwotnego i wykonać pomiary: rezystancji uziemień, sprawdzenie skuteczności ochrony przeciwporażeniowej, rezystancji izolacji kabli i ciągłości żył kabli.

6. Wszystkie prace ziemne oraz inne prace związane z wykorzystaniem sprzętu mechanicznego prowadzone w obrębie bryły korzeniowej drzew rosnących w bezpośrednim sąsiedztwie powinny być wykonywane w sposób najmniej szkodzącym drzewom i krzewom, zgodnie z art. 82 ust. 1 ustawy z dnia 16.04.2004 o ochronie przyrody (tekst jednolity; Dz.U. Z 2009r. Nr 151, poz. 1220 z późniejszymi zm.) w tym:

- wykopy wykonywane w obrębie stref korzeniowych drzew wykonać ręcznie poza okresem wegetacji,
- w przypadku odkrycia korzeni należy je zabezpieczyć.

10. Ochrona od porażen prądem elektrycznym

Z punktu widzenia ochrony przeciwporażeniowej sieć rozdzielcza na terenie kompleksu będzie pracować w układzie TN-S z odrębnym przewodem ochronnym PE i neutralnym N. Rozdział przewodu PEN na przewód PE i N nastąpi w rozdzielnicy głównej R.GŁ., punkt rozdziału należy uziemić.

Zbliżenia i skrzyżowania z istniejącymi i projektowaną infrastrukturą techniczną

Podczas prac ziemnych należy zachować normatywne odległości pomiędzy istniejącą i projektowaną infrastrukturą techniczną zgodnie z N-SEP-E-004 tablica nr: 2.. W projektowanych miejscach należy zastosować rury ochronne zgodnie z planszą zagospodarowania terenu. W przypadku odkrycia niezainwentaryzowanych sieci na terenie należy zastosować rury ochronne zgodnie z obowiązującymi przepisami.

11. Uziom budynku

Obowiązkowo należy wykonać uziom fundamentowy oraz połączenia wyrównawcze, których końce należy wyprowadzić do podłączenia szyny PE tablic licznikowych, miejscowych szyn wyrównawczych instalacji wod.-kan i C.O.

12. System kontroli dostępu KD

Ogólna koncepcja systemu

Kontroler o własne zasoby sprzętowe może obsługiwać do 4- przejść. Moduły rozszerzeń są dołączane do kontrolera za pośrednictwem magistrali RS485 z wykorzystaniem protokołu EPSO 3 lub równoważnego. Magistrala ta może tworzyć strukturę gwiazdy i mieć długość do 1200 m, licząc od kontrolera do najbardziej odległego modułu. Kontroler może również współpracować z urządzeniami podłączonymi do sieci komputerowej, który pełni rolę interfejsu komunikacyjnego do urządzeń sieciowych.

Przesyłanie ustawień do kontrolerów jest realizowane w tle i nie zatrzymuje bieżącej pracy systemu. Czas przesyłania ustawień zwykle nie przekracza 1 minuty na każdy tysiąc aktywnych użytkowników systemu. Po zakończeniu przesyłania następuje przełączenie systemu na nowe ustawienia, w trakcie, którego system wstrzymuje pracę na kilka sekund.

System umożliwia zarządzanie użytkownikami w trybie online. W trybie tym, aktualizacja danych użytkownika następuje natychmiast po wykonaniu zmian w bazie danych systemu. Przesyłanie zaktualizowanych danych użytkownika nie zatrzymuje działania systemu i zwykle zajmuje kilka sekund. Zdarzenia zarejestrowane w systemie są na bieżąco pobierane z kontrolerów i zapisywane w bazie danych systemu. Pobieranie zdarzeń następuje automatycznie przez serwer komunikacyjny systemu i nie wymaga działania aplikacji zarządzającej systemem.

W przypadku braku połączenia z serwerem komunikacyjnym, kontrolery zapisują zdarzenia w swoich wewnętrznych buforach pamięci. Zasoby sprzętowe kontrolera dostępu mogą być rozszerzane przez dołączanie zewnętrznych modułów i urządzeń. Zewnętrzne zasoby sprzętowe mogą być wykorzystywane wg tych samych zasad, co zasoby płyty głównej kontrolera. Lokalizacja obiektu (linii wejściowej, linii wyjściowej, czytnika itd.), jak i jego rodzaj (typ linii wejściowej, typ linii wyjściowej, typ czytnika) nie mają wpływu na funkcję logiczną, jaką można powiązać z danym obiektem fizycznym.

Kontroler

W zależności od wersji, kontroler MC16 lub równoważny umożliwia obsługę 16 przejść kontrolowanych dwustronnie oraz 32 węzłów automatyki. Koncepcja integracji z systemem alarmowym umożliwia prezentację stanu strefy alarmowej oraz sterowanie jej stanem bezpośrednio z poziomu terminali dostępu. Kontroler udostępnia zaawansowany, a jednocześnie bardzo wydajny sposób zarządzania użytkownikami systemu oraz kształtowania ich uprawnień. Proces konfiguracji kontrolerów systemu jest realizowany współbieżnie, a ilość kontrolerów w systemie nie wpływa na czas jego konfiguracji, który zwykle kończy się przed upływem 1 minuty. Kontroler zarządzany jest z aplikacji narzędziowej, która umożliwia współpracę z serwerową bazą danych Microsoft SQL Server oraz darmową bazą plikową Microsoft SQL Server Compact. Zarządzanie systemem może być realizowane z poziomu wielu stacji roboczych z programem narzędziowym VISO ST lub równoważnym i przez operatorów o różnym poziomie uprawnień. System RACS 5 lub równoważny udostępnia serwer integracji programowej umożliwiający swobodny dostęp do logu zdarzeń systemu jak i zarządzanie jego użytkownikami. Komunikacja z komputerem zarządzającym jest realizowana za pośrednictwem sieci LAN/WAN z protokołem szyfrowanym metodą AES128 CBC.

Terminal dostępu

Terminal MCT lub równoważny jest terminalem identyfikacji przeznaczonym do wykorzystania w systemie kontroli dostępu i automatyki budynkowej. Terminale MCT w zależności od wersji umożliwiają rozpoznawanie użytkowników za pośrednictwem kart zbliżeniowych standardu 13,56 MHz MIFARE® Ultralight/Classic/DESFire/PLUS, a także za pośrednictwem urządzenia mobilnego (telefonu) wyposażonego w technologię NFC lub Bluetooth oraz kodu PIN.

W przypadku identyfikacji przy wykorzystaniu technologii Bluetooth zasięg odczytu może sięgać do kilku metrów. Pozostałe metody wymagają zbliżenia identyfikatora do czytnika na odległość kilku centymetrów. Identyfikacja mobilna wymaga zainstalowania w telefonie aplikacji Roger Mobile Key lub równoważnej dostępnej dla systemu iOS oraz Android.

Czytnik MCT lub równoważny może być wyposażony w klawiaturę lub w dwa klawisze funkcyjne oznaczone symbolami Dzwonek i Światło, które alternatywnie mogą być wykorzystane do innych celów niż wskazują powiązane z nimi symbole. Posiada interfejs RS485 za pośrednictwem, którego jest podłączany do magistrali komunikacyjnej kontrolera.

Bezpieczeństwo w systemie

System oferuje wysoki, wielopoziomowy system bezpieczeństwa, na który składają się:

Zastosowanie kart standardu MIFARE® z programowalnym numerem zapisanym w szyfrowanych sektorach karty (SSN - Secure Sector Number).

Obsługa kart MIFARE® DESFire® i MIFARE Plus® oraz technologii mobilnej NFC/BLE.

Złożone Tryby logowania wymagające użycia kombinacji identyfikatorów (np. karta + PIN).

Komunikacja w sieci LAN/WAN szyfrowana metodą AES128 z dynamicznie zmienianym kluczem szyfrującym (CBC).

Szyfrowana komunikacja z terminalami dostępu i ekspanderami dołączonymi do magistrali RS485 z wykorzystaniem protokołu EPSO 3 lub równoważnego.

Autoryzacja zewnętrzna system umożliwia uzależnienie zgody na dostęp na konkretnym punkcie logowania od decyzji zewnętrznej. Decyzja ta może być wydana przez operatora monitorującego system VISO ST lub równoważny lub z poziomu dedykowanego do tego celu punktu logowania (czytnika).

Przykładowe funkcje systemu

Kontrola dostępu do pomieszczeń

Głównym zadaniem systemu jest realizacja fizycznej kontroli dostępu do pomieszczeń. System jest skalowalny i umożliwia obsługę nieograniczonej ilości przejść. Przejścia mogą być kontrolowane jedno lub dwustronnie. Ilość użytkowników systemu nie jest ograniczona. Ograniczeniu podlega ilość użytkowników na poszczególnych kontrolerach dostępu. System przesyła do kontrolera tylko tych użytkowników, którzy posiadają uprawnienie do wykonania jakiegokolwiek akcji na danym kontrolerze.

Raportowanie czasu obecności

System rejestruje zdarzenia związane z ruchem użytkowników na terenie objętym elektroniczną kontrolą dostępu. Rejestr zdarzeń może być wykorzystany do analizy czasu przebywania użytkowników w poszczególnych częściach dozorowanego obiektu. Program narzędziowy umożliwia wyznaczenie czasu przebywania użytkowników w dowolnie zdefiniowanych obszarach systemu (tzw. strefy obecności) i w dowolnym zakresie czasowym. Raportowanie czasu

obecności osób może odbywać się przez sumowanie częściowych czasów przebywania w określonym obszarze lub jako czas, który upłynął od momentu pierwszego wejścia aż do momentu ostatniego wyjścia z obszaru w ramach tego samego dnia.

Integracja z telewizją przemysłową

W ramach integracji z telewizją przemysłową CCTV system udostępnia możliwość pobrania i odtworzenia filmu lub zdjęcia zarejestrowanego przez kamerę skojarzoną z danym typem zdarzenia oraz miejscem jego wystąpienia. Opcjonalnie, film lub zdjęcie pobrane z rejestratora może zostać zachowane w bazie danych systemu. Podgląd z kamer może odbywać się w osobnym oknie programu zadokowanym na dodatkowym monitorze. Okno z podglądem kamery może się automatycznie przełączać na tą kamerę, która jest skojarzona z ostatnio zarejestrowanym zdarzeniem. W programie narzędziowym zintegrowano obsługę rejestratorów CCTV oraz kamer zgodnych ze standardem ONVIF.

Awaryjne sterowanie przejściami

System umożliwia zarówno otwarcie jak i zablokowanie dowolnej grupy przejść w trybie awaryjnym. Tryb ten ma najwyższy priorytet i nie może być zmieniony przez żaden inny dostępny w systemie mechanizm za wyjątkiem dedykowanej do tego celu funkcji kasującej tryb awaryjny. Sterowanie trybem awaryjnym przejścia może być realizowane zarówno lokalnie z poziomu urządzeń systemu, jak i zdalnie z programu narzędziowego.

Rejestracja zdarzeń

Zdarzenia, które wystąpiły w systemie są na bieżąco ściągane z kontrolerów i zapisywane w bazie danych systemu. Proces ściągania jest realizowany przez Serwer komunikacyjny, który jest usługą systemu operacyjnego Windows i nie wymaga uruchomienia programu narzędziowego zarządzającego systemem. W przypadku, gdy połączenie z kontrolerem jest nieosiągalne, zdarzenia są rejestrowane w wewnętrznym buforze zdarzeń kontrolera i są pobierane automatycznie po przywróceniu komunikacji.

Powiadamianie o wystąpieniu zdarzenia

Wystąpienie dowolnego zdarzenia może automatycznie uruchamiać akcję powiadomienia. Powiadomienie może odbywać się przez wyświetlenie komunikatu na ekranie monitora, wysłanie wiadomości email lub wysłanie pakietów danych przy pomocy protokołu TCP pod zdefiniowany adres sieciowy. Korzystając z uniwersalnego mechanizmu filtru zdarzeń można określić dodatkowe warunki (m.in. czas i miejsce wystąpienia zdarzenia), które muszą wystąpić, aby system wykonał powiadomienie. Powiadamianie protokołem TCP może być użyte to integracji programowej z innymi rodzajami programów (np. BMS).

Monitorowanie zdarzeń

Zdarzenia, które wystąpiły w systemie mogą być na bieżąco wyświetlane w oknach Monitorowania online. Każde z okien może być skonfigurowane do wyświetlania wybranej grupy zdarzeń i dokowane na dodatkowych monitorach.

Monitorowanie obecności

System umożliwia monitorowanie osób zalogowanych w dowolnie zdefiniowanych obszarach systemu. Możliwe jest monitorowanie wielu obszarów jednocześnie. W szczególnym przypadku monitor obecności może być użyty w celu prezentacji listy osób, które zarejestrowały się na wybranym punkcie dostępu w następstwie ogłoszenia ewakuacji budynku.

Monitorowanie przejść

System umożliwia monitorowanie wybranych przejść i podgląd zdarzeń, które na nich wystąpiły. W momencie wystąpienia zdarzenia system może automatycznie wyświetlić podgląd z kamery CCTV skojarzonej z miejscem wystąpienia zdarzenia lub zdjęcie osoby, która została zarejestrowana na tym miejscu.

Mapy

W systemie można definiować Mapy bazujące na dowolnych podkładach graficznych i nanosić na nie w procesie konfiguracji symbole reprezentujące wybrane elementy systemu (m.in. Przejścia, Punkty logowania, kamery CCTV). Z poziomu widoku Mapy możliwe jest wywołanie podglądu na żywo z kamery skojarzonej z danym symbolem jak też wykonanie komendy zdalnej.

Harmonogramy

Harmonogramy umożliwiają uzależnienie działania systemu od konkretnego dnia tygodnia i pory dnia. Harmonogramy mogą być wykorzystane przy konfigurowaniu działania wielu funkcji systemu, a w szczególności uprawnień

dostępu. Stan harmonogramu może być prezentowany na linii wyjściowej i umożliwić w ten sposób sprzętowe uzależnienie działania systemu od dnia tygodnia i pory dnia.

Uprawnienia

W systemie wykonanie dowolnej akcji może być uwarunkowane wymogiem posiadania właściwego Uprawnienia. Uprawnienie określa, kiedy i gdzie dana akcja (funkcja) może być wykonana. Uprawnienia mogą być przypisywane bezpośrednio do Identyfikatora, Użytkownika lub Grupy użytkowników. Uprawnienia przypisane do Grupy dostępu przechodzą automatycznie na wszystkich Użytkowników należących do danej Grupy. Uprawnienia przypisane do Identyfikatora automatycznie przechodzą na Użytkownika, do którego dany Identyfikator należy.

Szczególne cechy systemu kontroli dostępu:

- możliwość definiowania wielofunkcyjnych linii wejściowych
- możliwość definiowania wielofunkcyjnych linii wyjściowych (z możliwością ustawienia priorytetu dla funkcji)
- możliwość definiowania sposobu modulacji linii wyjściowej
- możliwość zastosowania czytników obsługujących standard BLE, NFC podłączanych do kontrolera po szyfrowanej magistrali RS485
- definiowanie własnych trybów logowania
- logowanie zwykłe, specjalne (długie przyłożenie karty – czas definiowany), podwójne; na jednym punkcie logowania możliwość wywoływania wielu funkcji
- komendy globalne wywoływane: dowolnym zdarzeniem w systemie, komendą ze stacji roboczej, aplikacji VISO Mobile lub równoważnej
- autoryzacja zewnętrzna (potwierdzenie tożsamości na ekranie Ochrony)

13. System monitoringu CCTV

Instalację CCTV projektuje się w oparciu o rejestrator, który należy zainstalować w projektowanej szafie dystrybucyjnej PPD.H3 (budynek bosmanatu). Projektuje się system monitoringu CCTV oparty na kamerach IP z matrycą min. 2Mpxl z zintegrowanym naświetlaczem IR i zasilanych PoE. Do kamer należy prowadzić przewód typu UTP 4x2x0.57 kat. 5E. Przewody należy zakończyć na pach panelach w szafie PPD.x. Dla zarządzania zapisem i podglądem obrazu służy dedykowane oprogramowanie.

Rejestracja

Ze względu na konieczność jednoznacznej i łatwej identyfikacji osób, zaprojektowano kamery kolorowe o wysokiej rozdzielczości. Systemem rejestracji wideo będzie serwer sieciowy, umożliwiający równoczesne nagrywanie kanałów wizyjnych w różnych rozdzielczościach NVR. System będzie umożliwiał podgląd obrazów „na żywo” oraz odtwarzanie materiału wcześniej nagranych. Zaprojektowany system przewidziano w taki sposób, by mógł w przyszłości obsługiwać strumienie wideo z istniejących kamer IP zlokalizowanych na innych obiektach inwestora. Zaprojektowano zapis z kamer w rozdzielczości min. 4mpix dla kamer tubowych kopułowych przy zastosowaniu kodeka H.265 z poklatkowością w trybie ciągłym 12kl/s przy 50% detekcji ruchu zarówno w ciągu dnia i nocy przez okres 30 dni.

Architektura

System zbudowany musi być w architekturze klient- serwer w z zastosowaniem architektury rozproszonej serwerów z zasilaczami redundantnymi oraz macierzami DAS pracująca w trybie RAID 5 lub 6. Architektura taka minimalizuje ryzyko utraty rejestrowanych danych w przeciwieństwie do architektury z centralną macierzą rejestrującą. Aplikacja serwerowa platformy musi wspierać architekturę 64-bitową w celu zapewnienie maksymalizacji wykorzystanie zasobów serwerów np. zapewnić obsługę min. 320 kamer w rozdzielczości FullD w trybie zapisu ruchu na jednej jednostce serwerowej. System musi zapewniać wsparcie dla szerokiego zakresu kodowanie obrazu w tymi min: MJPEG, MPEG-2, MPEG-4, MxPEG, H.264, H.265. Ponadto musi istnieć hierarchiczna struktura serwerów, w której można wyróżnić serwer centralny tzw. serwer master, który zarządza główną bazą danych, zawierającą wszystkie informacje o systemie i konfiguracji komponentów platformy oraz serwer slave. Serwer master ten autoryzuje użytkowników i nadaje dostęp do platformy na podstawie predefiniowanych praw dostępu użytkownika oraz ustawień strefy bezpieczeństwa otrzymywanych w czasie logowania z poziomu stacji operatorskiej.

Serwer master zarządza następującymi komponentami platformy:

- grupami użytkowników oraz użytkownikami
- alarmami z poszczególnych serwerów
- makrami.
- uprawnieniami poszczególnych grup użytkowników
- układami widoków, multi-widoków wraz z przypisanymi do nich urządzeń z poszczególnych serwerów slave
- sekwencjami kamer
- harmonogramami nagrywania i archiwizacji.
- wtyczkami (Plug-in) odpowiadającymi za komunikację pomiędzy platformą, a systemami firm trzecich, takimi jak zewnętrzna analityka wideo, system ochrony obwodowej itd.
- modulem API HTTP łączącym platformę z dowolną aplikacją lub interfejsem, który został stworzony z jego wykorzystaniem w celu integracji z platformą
- przydzielonymi kamerami i koderami oraz archiwizowanie wideo / audio
- urządzeniami zewnętrznymi np. audio, wejście, wyjścia, porty szeregowo; sterowanie PTZ.

Platforma musi zapewnić obsługę min 30 producentów kamer, koderów na bazie autorskich dedykowanych protokołów tych producentów oraz w przypadku, aby zapewnić jak największą elastyczność oraz możliwość doboru jak najlepszego urządzenia spełniającego wymagania ekspozycji, transmisji itp. w danym punkcie kamerowym. W przypadku braku wspierania dedykowanego protokołu dopuszcza się możliwość stosowanie protokołów generycznych takich jak Onvif oraz PSIA w celu połączenia urządzenia z platformą. Wymagane jest obsługiwanie wbudowanych w kamerę algorytmów badania, jakości obrazu kamery w celu ułatwienia zarządzania wielokamerowymi poprzez automatyczne poinformowanie operatora, administratora o utracie jakości obrazu.

Serwer systemu CCTV IP musi zapewniać możliwość obsługi do 500 urządzeń w tym kamer, kanałów video z koderów video oraz obsługę połączenia kodera, dekodera, klawiatury CCTV IP i moduły we / wy. System musi zapewniać możliwość implementacji w systemie wirtualizacyjnym min. Vmware. Cecha ta zapewnia możliwość wykorzystania posiadanej przez inwestora infrastruktury serwerowej przy optymalizacji kosztowej wdrażanie systemu bezpieczeństwa oraz wykorzystanie dodatkowych oferowanych przez środowisko wirtualizacji funkcjonalności jak min. łatwa przywracanie systemów po awarii czy dynamiczna lustrzana kopia danych. System musi gwarantować najwyższy poziom bezpieczeństwa danych w warstwie sprzętowej serwera, usługi systemu operacyjnego, aplikacyjnej – przez możliwość wdrożenia w systemie serwera redundantnego, detekcję sabotażu punktu kamerowego, watchdog aplikacji oraz redundancję sprzętową. Platforma musi zapewniać możliwość wykorzystania aplikacyjnego serwera redundantnego. Serwer redundantny jest dedykowanym serwerem, którego rolą jest permanentny monitoring stanu działania wszystkich serwerów platformy w celu przeciwdziałania utracie następujących możliwości w przypadku uszkodzenia lub nieprawidłowego funkcjonowanie jednego z serwerów: archiwizacji materiału oraz odtworzeniu w przyszłości z okresu trwania awarii podglądu na żywo z kamer w czasie trwania awarii

Serwer monitoruje stan serwerów na następujących warstwach:

sprzętowej – sprawdzanie prawidłowego funkcjonowania podsystemu dyskowego, karty sieciowej, zasilania
 aplikacyjnej – sprawdzanie stanu aplikacji na serwerach nagrywających

System powinien umożliwiać dokonywanie kopii ustawień serwerów tzn codzienne o ustalonej godzinie (np. o godz. 24: 00) wykonywanie kopii zapasową ustawień monitorowanych serwerów przez serwer redundantny – ma to na celu doprowadzenie do sytuacji, aby w przypadku przejścia roli uszkodzonego serwera serwer ten posiadał najaktualniejszą konfigurację serwera uszkodzonego serwera. Zaprojektowano możliwość przejścia roli uszkodzonego serwera - jeżeli na jakiegokolwiek z wymienionych płaszczyzn serwer redundantny zarejestruje problem w czasie od 90 sekund przejmie wszystkie funkcjonalności serwera, z którym zaistniał problem. Serwer redundantny nie zmienia adresu IP, zatem gdy rozpoczyna swoją pracę w miejsce serwera uszkodzonego informuje wszystkie stacje klienckie, iż przejął jego rolę i aby od tego czasu stacje kontaktowały się z nim. Gdy serwer uszkodzony zostanie naprawiony lub gdy zostanie przywrócona do prawidłowego funkcjonowania aplikacja na wadliwie działającym serwerze serwer redundantny odwraca wcześniejszy proces oraz powraca w tryb nasłuchiwanie oddając swoją tymczasową rolę przywróconemu serwerowi. Cały proces odbywa się automatycznie.

Obsługa serwera redundantnego – serwer redundantny nie wymaga od operatora jakiegokolwiek ingerencji zarówno w celu:

uzyskanie obrazu na żywo z kamer uzyskanie materiału archiwalnego z kamer dotychczas obsługiwanych przez niesprawny serwer.

Obraz na żywo zostaje przywrócony po czasie ok. do 90 sekund od wystąpienia awarii, czyli po czasie koniecznym do zainicjalizowania serwera redundantnego ustawieniami serwera uszkodzonego – do tego czasu w panelach obrazu na żywo z kamer zostanie wyświetlona informacja o utracie kontaktu z serwerem.

Odtwarzanie materiału archiwalnego z okresu wystąpienia awarii nie różni się w żaden sposób od obsługi materiału z okresu prawidłowego funkcjonowania serwera oryginalnego. Dostęp do materiału zgromadzonego na serwerze redundantnym odbywa się za pomocą odpowiednich meta-danych wskazujących ścieżkę zapisu materiału w czasie wystąpienia awarii – jest on realizowany przez dedykowany wątek aplikacji i dla operatora jest całkowicie transparentny.

Watchdog usługi serwerowej platformy – w celu eliminacji negatywnego wpływu innych aplikacji współdzielących system operacyjny aplikacja serwera musi być realizowana na bazie usługi systemowej. Ponadto na wypadek zaistnienia negatywnego wpływu systemu operacyjnego usługa serwera ma być wspierana przez aplikację / usługę typu Watchdog, której celem jest monitorowanie usługi serwerowej w celu zagwarantowania, iż system jest cały czas w stanie stabilnej pracy.

Odbywa się to poprzez sprawdzanie kilku newralgicznych podsystemów:

- prawidłowego niezakleszczonego stan usługi serwerowej
- prawidłowego działania macierzy dyskowej RAID 5/ 6
- prawidłowego działania bazy danych

W przypadku wykrycia nieprawidłowości usługa serwerowa jest restartowana w celu uniknięcia błędnego funkcjonowania części platformy w dłuższym czasie, co mogłoby spowodować brak możliwości nagrywania w przypadku serwerów rejestrujących lub braku możliwości podglądu obrazów na żywo, interaktywnej obsługi systemu w przypadku stacji operatorskich.

Anty-sabotaż punktu kamerowego - dla każdego punktu kamerowego możliwe będzie bez konieczności wykupu dodatkowej licencji detekcja sabotażu punktu kamerowego dokonywana przez serwer. Funkcje analizy obrazu są wspomagane ciągłym monitorowaniem zakresu obserwowanej przez kamerę sceny. W przypadku zmiany kąta obserwacji, zakrycia obiektywu lub rozmycia obrazu system automatycznie informuje o tym fakcie operatora, co jest gwarantem poprawnego działania poszczególnych algorytmów wideo identyfikacji oraz wideo detekcji.

Serwer platformy CCTV IP zapewniać musi zabezpieczenie struktury danych video, audio oraz metadanych poprzez zastosowanie technologii RAID 6 w przypisanej do serwera macierzy dyskowej. W celu zapewnienia ciągłości pracy w przypadku uszkodzenia: dysku twardego, zasilacza lub modułów chłodzenia serwer ma zapewniać możliwość wymiany uszkodzonego podzespołu bez konieczności wyłączenia serwera i przerywania pracy platformy zarządzającej.

Parametry urządzeń systemu CCTV IP

Kamery tubowe

Zaprojektowano 4-megapikselowe kamery IP, zapewniające szczegółowe obrazy w każdej sytuacji. Kamera kompresuje wideo zgodnie z najnowszą technologią H.265. Dostępnych jest wiele opcji umożliwiających łatwą integrację kamery z systemem zarządzania wideo. Kamera wyposażona jest w bogaty zestaw inteligentnych czujników VCA, które pomagają operatorowi wykryć wszelkie anomalie. Zaproponowana kamera zawiera zestaw narzędzi do poprawy jakości obrazu, takich jak inteligentne IR, BLC i redukcja szumów 3D.

Zaprojektowaną kamerę tubową muszą cechować nie gorsze parametry :

Standard:	TCP/IP
Przetwornik:	1/3 " Progressive Scan CMOS
Wielkość matrycy:	4.0 Mpx
Rozdzielczość:	2560 x 1440 - 3.7 Mpx , 2304 x 1296 - 3.0 Mpx , 1920 x 1080 - 1080p 1280 x 720 - 720p
Tryby pracy:	Strumienie główny i pomocniczy mogą występować w dowolnej konfiguracji Firmware V5.5.53 build: 180716

	<ul style="list-style-type: none"> Strumień główny : 2560 x 1440, 2304 x 1296, 1920 x 1080, 1280 x 720 Strumień pomocniczy : 640 x 480, 640 x 360, 352 x 288
Obiektyw:	2.8 ... 12 mm - AutoFocus
Kąt widzenia:	98 ° ... 28 °
Kompresja:	H.265 / H.265+ / H.264 / H.264+ / MJPEG
Zasięg oświetlacza IR:	30 m
Wejścia / wyjścia alarmowe:	nie
Przepływność (bitrate):	32 ... 8192 kbit/s
Prędkość transmisji strumienia głównego:	20 kl/s @ 3.7 Mpx 25 kl/s @ 3.0 Mpx
Interfejs sieciowy:	10/100 Base-T(RJ-45)
Protokoły sieciowe:	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, NTP, UPnP, SMTP, IGMP, IEEE 802.1x, QoS, IPv6, UDP, Bonjour
Audio:	nie
WEB Server:	Wbudowany, Zgodność z NVR
Gniazdo karty pamięci:	Obsługa kart Micro SD do 128GB (możliwy zapis lokalny)
Dostęp z telefonu komórkowego:	Port: 8000 lub dostęp przez chmurę (P2P) <ul style="list-style-type: none"> Android: Darmowa aplikacja iVMS-4500 lub Hik-Connect iOS (iPhone): Darmowa aplikacja iVMS-4500 lub Hik-Connect
Domyślny login / hasło administratora:	admin / -
Domyślny adres IP:	192.168.1.64
Porty dostępu przez www:	80
Porty dostępu przez aplikację na PC:	Port: 8000 lub dostęp przez chmurę (P2P) - aplikacja iVMS-4200
Port dostępu przez aplikację mobilną:	8000
Port ONVIF:	80
RTSP URL:	<ul style="list-style-type: none"> Strumień główny rtsp://192.168.1.64:554/Streaming/Channels/101/ - RTSP - bez autoryzacji rtsp://uzytkownik:haslo@192.168.1.64:554/Streaming/Channels/101/ - z autoryzacją Strumień pomocniczy rtsp://192.168.1.64:554/Streaming/Channels/102/ - RTSP - bez autoryzacji rtsp://uzytkownik:haslo@192.168.1.64:554/Streaming/Channels/102/ - z autoryzacją

Interfejs RS-485:	nie
Maks. liczba użytkowników on-line:	6
Wybrane funkcje:	<ul style="list-style-type: none"> • WDR - 120 dB - Szeroki zakres dynamiki oświetlenia • 3D-DNR - Cyfrowa redukcja szumu w obrazie • ROI - poprawianie jakości wybranych fragmentów obrazu • Anti-Flicker - Technologia eliminująca męczący oczy efekt migotania obrazu • AGC - Automatyczna regulacja wzmocnienia obrazu • WB - Balans bieli (ATW/AWB/manualny/wewnętrzny/zewnętrzny) • BLC - konfigurowalna kompensacja światła wstecznego • ICR - Mechaniczny filtr podczerwieni • Tryb dzień/noc (color/b&w/auto) • Detekcja ruchu • Konfigurowalne strefy prywatności • Mirror - Odbicie lustrzane obrazu • Sharpness - Wyost్రzanie konturów obrazu
Zasilanie:	<ul style="list-style-type: none"> • PoE (802.3af), • 12 V DC / 900 mA
Pobór mocy:	<div> <div>≤ 12.9 W @ PoE (802.3af)</div> <div>≤ 11 W @ 12 V DC</div> </div>
Temperatura pracy :	-30 °C ... 60 °C
Obudowa:	Compact, Metalowa
Kolor:	Biały
Klasa szczelności:	IP67
Obsługiwane języki:	polski, angielski, francuski, hiszpański, portugalski, rosyjski, turecki, włoski
Waga:	0.72 kg
Wymiary:	Ø 105 x 245
Producent / Marka:	HIKVISION

Kamery kopułkowe

Zaprojektowano 4-megapikselowe kamery kopułkowe IP, zapewniające wyraźne obrazy w każdej sytuacji. Inteligentne kodowanie wideo zapewnia bardzo dobrą jakość obrazu i niskie koszty przechowywania. Kamera kompresuje wideo zgodnie z najnowszą technologią H.265. Posiada funkcję wielostrumieniową do jednoczesnego przesyłania strumieniowego w formatach H.265, H.264 i MJPEG. Dostępnych jest wiele opcji umożliwiających łatwą integrację kamery z systemem zarządzania wideo. Kamera wyposażona jest w bogaty zestaw inteligentnych czujników VCA, które pomagają operatorowi wykryć wszelkie anomalie.

Zaprojektowaną kamerę kopułkową muszą cechować nie gorsze parametry :

tandard:	TCP/IP
Przetwornik:	1/3 " Progressive Scan CMOS

Wielkość matrycy:	4.1 Mpx
System skanowania:	Progresywny
Rozdzielczość:	2688 x 1520 - 4.0 Mpx , 2560 x 1440 - 3.7 Mpx , 2304 x 1296 - 3 Mpx , 1920 x 1080 - 1080p
Tryby pracy:	Strumienie główny i pomocniczy mogą występować w dowolnej konfiguracji Firmware V5.5.51 build 180314 <ul style="list-style-type: none"> • Strumień główny : 2688 x 1520, 2560 x 1440, 2304 x 1296, 1920 x 1080 • Strumień pomocniczy : 640 x 480, 640 x 360, 320 x 240 • Strumień pomocniczy 2 : 1280 x 720, 640 x 360, 352 x 288
Obiektyw:	2.8 mm
Kąt widzenia:	<ul style="list-style-type: none"> • 103 ° (dane producenta) • 100 ° (nasze testy)
Zasięg oświetlacza IR:	30 m
Stosunek sygnał/szum (S/N):	> 50 dB
Interfejs RS-485:	brak
Metoda kompresji obrazu:	H.265 / H.265+ / H.264 / H.264+ / MJPEG
Wejścia / wyjścia alarmowe:	1 / 1
Audio:	<ul style="list-style-type: none"> • Wejście na mikrofon zewnętrzny • Wyjście audio • Obsługa dwukierunkowego audio
Gniazdo karty pamięci:	Obsługa kart Micro SD do 128GB (możliwy zapis lokalny)
Przepływność (bitrate):	256 ... 16384 kbit/s
Prędkość transmisji strumienia głównego:	25 kl/s @ 4.0 Mpx
Interfejs sieciowy:	10/100 Base-T(RJ-45)
Protokoły sieciowe:	TCP/IP, UDP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, IEEE 802.1x, QoS, IPv6, Bonjour
WEB Server:	Wbudowany
Maks. liczba użytkowników on-line:	6
ONVIF:	16.12
Dostęp z telefonu	Port: 8000 lub dostęp przez chmurę (P2P)

komórkowego:	<ul style="list-style-type: none"> • Android: Darmowa aplikacja iVMS-4500 lub Hik-Connect • iOS (iPhone): Darmowa aplikacja iVMS-4500 lub Hik-Connect
Domyślny login / hasło administratora:	admin / - Hasło administratora należy ustawić przy pierwszym uruchomieniu
Domyślny adres IP:	192.168.1.64
Porty dostępu przez www:	80
Porty dostępu przez aplikację na PC:	Port: 8000 lub dostęp przez chmurę (P2P) - aplikacja iVMS-4200
Port dostępu przez aplikację mobilną:	8000
Port ONVIF:	80
RTSP URL:	<ul style="list-style-type: none"> • Strumień główny rtsp://192.168.1.64:554/Streaming/Channels/101/ - RTSP - bez autoryzacji rtsp://użytkownik:hasło@192.168.1.64:554/Streaming/Channels/101/ - z autoryzacją • Strumień pomocniczy rtsp://192.168.1.64:554/Streaming/Channels/102/ - RTSP - bez autoryzacji rtsp://użytkownik:hasło@192.168.1.64:554/Streaming/Channels/102/ - z autoryzacją
Wybrane funkcje:	<ul style="list-style-type: none"> • WDR - 120 dB - Szeroki zakres dynamiki oświetlenia • 3D-DNR - Cyfrowa redukcja szumu w obrazie • ROI - poprawianie jakości wybranych fragmentów obrazu • ANR - zapis obrazu na karcie przy braku łączności z rejestratorem (awaria sieci) oraz późniejsza synchronizacja • BLC/HLC - kompensacja światła tła / silnego światła • Przycisk RESET • Możliwość zmiany rozdzielczości, jakości i przepustowości • Konfigurowalne strefy prywatności • Mirror - Odbicie lustrzane obrazu • Sharpness - Wyostrażanie konturów obrazu • Analiza obrazu : Detekcja ruchu, wtargnięcie, przekroczenie linii, detekcja twarzy
Zasilanie:	<ul style="list-style-type: none"> • PoE (802.3af), • 12 V DC / 500 mA
Pobór mocy:	$\leq 6 \text{ W}$ @ 12 V DC $\leq 7.5 \text{ W @ PoE (802.3af)}$
Obudowa:	Dome, Metalowa
Wandaloodporna:	IK10
Klasa szczelności:	IP67
Kolor:	Biały
Temperatura pracy :	-30 °C ... 60 °C

Waga:	0.6 kg
Wymiary:	Ø 111 x 82 mm
Obsługiwane języki:	polski, angielski, bułgarski, chorwacki, czeski, duński, estoński, fiński, francuski, grecki, hiszpański, holenderski, litewski, łotewski, niemiecki, norweski, portugalski, rosyjski, rumuński, serbski, słowacki, słoweński, szwedzki, turecki, węgierski, wietnamski, włoski
Producent / Marka:	HIKVISION

Serwer

Zaprojektowano wydajny i konfigurowalny serwerem NVR z możliwością montażu typu rack. Serwer zaprojektowano w szafie PPD znajdującej się pomieszczeniu Serwerowni. Przewidziano serwer, który jest połączeniem wysokiej wydajności komponentów z przyjazną użytkownikowi konfiguracją zapewniając wysoką moc i niezawodność. Obudowa i komponenty są tak zaprojektowane aby zapewnić optymalny przepływ powietrza dla większej wydajności, co powoduje mniejsze zużycie energii. Jego redundantny zasilacz zapewnia ciągłą pracę przez cały czas. Serwer powinien cechować parametry o wartościach nie gorszych niż :

wejścia audio / wideo	
Ilość obsługiwanych kanałów	128
Pasmo przychodzące / wychodzące	576 Mbps/512 Mbps
Pasmo przychodzące / wychodzące (RAID)	576 Mbps/512 Mbps
Wspierane protokoły	HIKVISION, ACTi, ARECONT, AXIS, BOSCH, BRICKCOM, CANON, HUNT, ONVIF (wersja 2.5), PANASONIC, PELCO, PSIA, RTSP, SAMSUNG, SONY, VIVOTEK, ZAVIO
Wyjścia audio / wideo	
Wyjście HDMI	Dwa niezależne wyjścia HDMI o rozdzielczości: 4K (4096 × 2160)/30Hz, 4K (3840 × 2160)/60Hz, 2K (2560 × 1440)/60Hz, 1080p (1920 × 1080)/60Hz, UXGA (1600 × 1200)/60Hz, SXGA (1280 × 1024)/60Hz, 720p (1280 × 720)/60Hz, XGA (1024 × 768)/60Hz
Wyjście VGA	1szt. Obsługiwane rozdzielczości: 1080p (1920 × 1080)/60Hz, UXGA (1600 × 1200)/60Hz, SXGA (1280 × 1024)/60Hz, 720p (1280 × 720)/60Hz, XGA (1024 × 768)/60Hz
Wyjście audio	1 kanał, RCA (2.0 Vp-p, 1 KΩ)
Dekodowanie audio / wideo	
Wspierane kompresje	H.265, H.265+, H.264, H.264+, MPEG4, MJPEG (tylko dla kamer Hikvision)
Obsługiwane rozdzielczości zapisu	12 MP / 8 MP / 7 MP / 6 MP / 5 MP / 4 MP / 3 MP / 1080p / UXGA / 720p / VGA / 4CIF / DCIF / 2CIF / CIF / QCIF
Jednoczesne odtwarzanie	Do 16 kanałów
Wydajność odtwarzania	3CH@12MP (30fps), 5CH@8MP (30fps), 6CH@6MP (30fps), 10CH@4MP (30fps), 20CH@2MP (30fps)

Dyski twarde	
Interfejsy SATA	16x SATA, hot-plug
Maksymalna pojemność	Do 10 TB na każdy z dysków
RAID	
Obsługiwane konfiguracje	RAID0, RAID1, RAID5, RAID 6, RAID10
Sieć	
Interfejsy sieciowe	4x RJ45 10M/100M/1000M, samoadaptacyjne
Protokoły	IPv6, HTTPS, UPnP, SNMP, NTP, SADP, SMTP, NFS, iSCSI, PPPoE, DDNS
Interfejsy	
Dwukierunkowe wejście audio	1 kanał, RCA (2.0 Vp-p, 1 KΩ)
Port szeregowy	1x RS-485, klawiatura
USB	Panel przedni: 2 × USB 2.0, Panel tylny: 2 × USB 3.0
Wejścia/wyjścia alarmowe	16/8
Ogólne	
Zasilanie	100 do 240 VAC, 550W
Wentylatory	Redundantny, podwójny wentylator z łożyskiem kulkowym, regulacja prędkości, hot-plug
Pobór mocy (bez HDD)	≤ 140W
Dopuszczalna temperatura pracy	0 °C do + 50 °C
Dopuszczalna wilgotność (bez skroplenia)	10% do 90%
Wysokość obudowy (rack)	3U
Wymiary (S × G × W)	442 × 494 × 146 mm
Waga (bez HDD)	≤ 16 kg

14. Instalacja teletechniczna zewnętrzna

Projektuje się wybudowanie kanalizacji kablowej, ze studniami dostępowymi. Kanalizację pierwotną należy wybudować z rur typu RHDPE 110/6,3mm. Budowa przeprowadzona zostanie metodą przecisku/przewiertu pod nawierzchniami utwardzonymi (jezdnie asfaltowe, chodniki z polbruku) zaś w terenie nieutwardzonym wykopem otwartym. Projektowane rury rozbudowywanej kanalizacji należy wprowadzić do projektowanych studni kablowych. Głębokość ułożenia kanalizacji powinna być taka, aby najmniejsze przykrycie liczone od poziomu nawierzchni wynosiło min. 0,7m a pod wjazdami na posesje, zjazdami w boczne uliczki, w pobliżu drzew i pod drogą min 0,8m (należy dostosować się do istniejących rzędnych terenu i ulicy). Przed ułożeniem rur kanalizacji kablowej dno rowu kablowego powinno być oczyszczone z kamieni i innych przedmiotów oraz starannie wyrównane. Rury kanalizacji kablowej układane w wykopie powinny być zasypywane najpierw warstwą piasku lub miłkłej ziemi o grubości, co najmniej 10 cm nad powierzchnią rur. Przyłącze ułożone w ziemi należy na całej długości oznaczyć taśmą ostrzegawczą w kolorze żółtym.

15. Obliczenia techniczne

- Spadki napięć na instalacjach wewnętrznych zgodnie z normą.
- Czasy wyłączenia prądów zwarciovych dla przyjętych średnic przewodów zachowane.
- Urządzenia dobrane na prądy zwarciove.

16. Uwagi końcowe

Całość instalacji wykonać zgodnie z obowiązującymi normami i przepisami z zachowaniem przepisów BHP.

- instalacje elektryczne układać po wykonaniu głównych robót budowlanych.
- wykonać pomiar rezystancji uziemienia w projektowanych złączach
- po wykonaniu instalacji dokonać niezbędnych pomiarów w tym:
- Pomiar impedancji pętli zwarcia
- Sprawdzenie ciągłości przewodów
- Pomiar rezystancji izolacji przewodów
- spadki napięcia oraz prądy zwarciove zgodnie z normą

Sprawdził: mgr inż. Mariusz Piątkowski
upr. proj. ZAP/0125/PWOE/11

Projektował: mgr inż. Piotr Markowski
upr. proj. ZAP/0218/POOE/11

.....

.....