

## PROJEKT TECHNICZNY

Nazwa: **Przebudowa, remont oraz zmiana sposobu użytkowania budynku służby zdrowia (przychodnia) na budynek kultury (muzeum) wraz z jego rozbudową o schody zewnętrzne oraz budową tablicy informacyjnej (ekranu ledowego), ogrodzenia, opaski wokół budynku, miejsca na gromadzenie odpadów stałych wraz z osłoną (utwardzonego placu do ustawiania kontenerów z zamykanymi otworami wrzutowymi), utwardzonego placu pod agregaty klimatyzacyjne wraz z osłoną, instalacji wewnętrznych: wentylacji mechanicznej, wodno-kanalizacyjnej, centralnego ogrzewania, elektrycznej, słaboprądowej oraz budowie instalacji odgromowej na działce nr 82/1 i 82/2 (obr. 0050, ark. 60) położonej przy ul. Okulickiego 9 w Radomiu.**

Adres: **ul. gen. Leopolda Okulickiego 9, Radom 26-600**

Numer działki: **82/1, 82,2 obr. 0050 Radom**

Kategoria obiektu budowlanego: **XI**

Inwestor: **Muzeum im. Jacka Malczewskiego,  
26-600 Radom, Rynek 11**

Branża: **Elektryczna i słaboprądowa**

Data: **Grudzień 2023**

Branża	Imię i Nazwisko	Nr uprawnień	Podpis
Projektant: Instalacje elektryczne	Rafał Góra	MAP/0315/POOE/13	
Sprawdzający: Instalacje elektryczne	Wiesław Dzierwa	BPP-Upr. 336/82	

## SPIS TREŚCI

### OPIS TECHNICZNY

1. WSTĘP	str. 3
2. PODSTAWA OPRACOWANIA	str. 3
3. ZASILANIE I POMIAR ENERGII	str. 3
4. WLZ I TABLICE ROZDZIELCZE	str. 4
5. INSTALACJA OŚWIETLENIA I GNIAZD WTYKOWYCH	str. 5
6. INSTALACJA OŚWIETLENIA EWAKUACYJNEGO	str. 5
7. INSTALACJA ZASILANIA KOMPUTEROWEGO	str. 6
8. INSTALACJA SIŁY I ZASILANIA ODBIORNIKÓW TECHNOLOGICZNYCH	str. 6
9. INSTALACJA POŁĄCZEŃ WYRÓWNAWCZYCH	str. 7
10. OCHRONA PRZECIWPORAŻENIOWA	str. 7
11. OCHRONA PRZECIWPRZEPięCIOWA	str. 8
12. INSTALACJA ODGROMOWA	str. 8
13. INSTALACJA OKABLOWANIA STRUKTURALNEGO	str. 8
14. INSTALACJA SYGNALIZACJI POŻARU	str. 18
15. INSTALACJA STEROWANIA ODDYMIANIEM	str. 32
16. SYSTEM ZARZĄDZANIA INSTALACJAMI BEZPIECZEŃSTWA – SMS	str. 33
17. INSTALACJA KONTROLI DOSTĘPU KD	str. 37
18. INSTALACJA TELEWIZJI DOZOROWEJ	str. 42
19. INSTALACJA SYGNALIZACJI WŁAMANIA I NAPADU	str. 62
20. INSTALACJA MULTIMEDIALNA	str. 70
21. SYSTEM DETEKЦИИ WYCIEKU	str. 77
22. SYSTEM PRZYWOŁAWCZY	str. 80
23. UWAGI KOŃCOWE	str. 80
OBLICZENIA	str. 81
INFORMACJA BIOZ	str. 83

### 1. WSTĘP

Przedmiotem niniejszego opracowania jest projekt techniczny instalacji elektrycznych i słabo prądowych dla przebudowy, remontu oraz zmiany sposobu użytkowania budynku służby zdrowia (przychodnia) na budynek kultury (muzeum) wraz z jego rozbudową o schody zewnętrzne oraz budową tablicy informacyjnej (ekranu ledowego), ogrodzenia, opaski wokół budynku, miejsca na gromadzenie odpadów stałych wraz z osłoną (utwardzonego placu do ustawiania kontenerów z zamykanymi otworami wrzutowymi), utwardzonego placu pod agregaty klimatyzacyjne wraz z osłoną, instalacji wewnętrznych: wentylacji mechanicznej, wodno-kanalizacyjnej, centralnego ogrzewania, elektrycznej, słaboprądowej oraz budowie instalacji odgromowej na działce nr 82/1 i 82/2 (obr. 0050, ark. 60) położonej przy ul. Okulickiego 9 w Radomiu.

### 2. PODSTAWA OPRACOWANIA

Projekt opracowano na podstawie:

- zlecenie Inwestora;
- warunki przyłączenia wydane przez TAURON S.A.;
- podkłady architektoniczne;
- uzgodnienia międzybranżowe;
- obowiązujące normy i przepisy.

### 3. ZASILANIE I POMIAR ENERGII

Budynek zasilany będzie poprzez zestaw złączowo pomiarowy Z3+1PP zabudowany na zewnątrz budynku.

**Zestaw złączowo pomiarowy oraz przyłącze nie stanowią tematu niniejszego opracowania, poza zakresem opracowania.**

Wyłącznik główny (pożarowy) WG dla budynku zamontowany będzie obok (lub nad) zestawu złączowo pomiarowego. Wyłącznik WG należy zamówić jako certyfikowany przez CNBOP zestaw Przeciwpóźarowego Wyłącznika Prądu.

Zestaw przeciw pożarowego wyłącznika prądu składa się z następujących elementów:

- Urządzenia wykonawczego UW (rozłącznik w głównym torze prądowym wraz z automatyką) (WG)
- Urządzenia uruchamiającego UU (przycisk z szybką przy wejściu do budynku) – UU PWP)
- Urządzenie sygnalizacyjnego US (lampka sygnalizacyjna przy wejściu do budynku) – US PWP)

Wyżej wymieniony zestaw powinien być w całości certyfikowany przez CNBOP.

Przycisk PWP UU i lampka sygnalizacyjna US będą zlokalizowane na zewnętrznej ścianie przy wejściu frontowym do budynku. Przycisk PWP UU będzie sterował z zadziałaniem wyzwalacza wzrostowego głównym Wyłącznikiem Prądu GWP w projektowanym wyłączniku WG. Zbicie szyby w PWP UU powoduje zadziałanie wyzwalacza wzrostowego i rozłączenie GWP. Zadziałanie GWP spowoduje odłączenie zasilania w całym obiekcie, poza zasilaniem urządzeń, których funkcjonowanie jest niezbędne w trakcie pożaru. Z przed wyłącznika WG wykonać zasilania

urządzeń wymagających działania w trakcie pożaru między innymi centralki SSP, zasilaczy pożarowych, centralki sterowania oddymiania. Zasilanie urządzeń działających w trakcie pożaru w budynku wykonać przewodami ognioodpornymi, bezhalogenowymi, np. typu NHXH PH90 lub podobnymi.

Stan położenia GWP jest wskazywany przez diody sygnalizacyjne na elewacji szafki PWP/UW i lampkę sygnalizacyjną PWP US przy wejściu do obiektu. Przycisk PWP UU jest wyposażony w optyczną sygnalizację jego stanu. Przyciski PWP UU powinny być wyposażone w szklaną szybkę, której zbitcie powoduje wyzwolenie wyłącznika.

Okablowanie zestawu WG należy wykonać przewodami zgodnie ze schematami. Podłączenie urządzeń uruchamiających oraz urządzeń sygnalizacyjnych należy wykonać przewodami o odporności ogniowej min. 90 min.

Wyłącznik WG zostanie zabudowane jako wolnostojąca przy ścianie elewacji.

W wyłączniku WG należy wykonać rozdział sieci z TN-C na TN-C-S. Rozdział PEN na PE i

N powinien być uziemiony poprzez przyłączenie do projektowanego uziemienia budynku.

W przypadku nie uzyskania wymaganej rezystancji uziemienia należy wykonać dodatkowo uziom pionowy. Wymagana wartość wypadkowej rezystancji uziemienia powinna być mniejsza od  $5\Omega$ .

Od zestawu złączowo pomiarowego do rozdzielni głównej RG w budynku, poprzez przełącznik 1-0-2 oraz wyłącznik główny WG należy ułożyć wewnętrzną linię zasilającą wykonaną przewodami WLZ-5xN2XH-J 1x95.

W projekcie ujęto okablowanie pod zasilanie rezerwowe z agregatu prądotwórczego pokrywające całe zapotrzebowanie energii elektrycznej obiektu w wypadku zaniku napięcia z sieci podstawowej. Załączanie agregatu odbywać się będzie ręcznie, za pomocą przełącznika (1-0-2).

UWAGA :Agregat poza zakresem opracowania.

#### **4. WLZ i TABLICE ROZDZIELCZE**

W piwnicy, zlokalizowana będzie rozdzielnia główna RG. Z rozdzielni tej wyprowadzona będzie wewnętrzna linia zasilająca rozdzielnie piętrowe (R1, R2), rozdzielnie serwerowni (RS) oraz tablice wymiennikowni (TMPEC). Rozdzielnice i tablice należy wykonać w obudowach naściennych lub wnękowych z drzwiczkami, zgodnie ze schematami ideowymi oraz widokami tablic.

Wewnętrzne linie zasilające należy układać w wyznaczonych szachtach, w przestrzeni międzystropowej w metalowych korytkach instalacyjnych, na uchwytych oraz pod tynkiem lub w posadzce, w winidurowych rurkach ochronnych. W budynku stosować korytka perforowane metalowe ocynkowana o ścianie 1mm, wysokość burty 60mm. Wszystkie korytka w budynku należy podwieszać w sposób trwały i pewny. Rozstaw podwieszonych dla koryt kablowych należy dostosować do nośności koryta przy założeniu jego maksymalnego obciążenia, jednak nie rzadziej niż 1,5m. W szachcie kable prowadzone będą na drabinach kablowych. Dla instalacji silno- i niskoprądowych zaprojektowano wydzielone koryta i drabiny kablowe. Kable pożarowe odchodzące z szachtu mocować za pomocą atestowanych uchwytych i obejm kablowych o odporności E90. Na trasach kablowych pożarowych dozwolone jest układanie jedynie kabli pożarowych o odporności ogniowej E90 typu NHXH i przewodów E90 typu HDGs. Instalacje pożarowe powinny przebiegać powyżej wszystkich palnych instalacji. Kable mocować w odstępach maksymalnie co 30cm.

UWAGA: Wszystkie przejścia przewodów przez strefy pożarowe i przez stropy należy zabezpieczyć masą ognioodporną o odporności równej odporności przegrody

## 5. INSTALACJA OŚWIETLENIA I GNIAZD WTYKOWYCH

Instalacje należy wykonać przewodami N2XH-J/YnDYżo, przekroje przewody zgodnie ze schematem ideowym tablicy. Należy zastosować osprzęt melaminowy podtynkowy, w sanitariatach oraz w pomieszczeniach technicznych - hermetyczny. Oświetlenie pomieszczeń wykonać oprawami z energooszczędnymi źródłami światła, rozmieszczonymi zgodnie z rysunkami. Sterowanie oświetleniem odbywać się za pomocą paneli sterowania (system DALI). Na poziomie piwnic oraz parteru, centralnie z panelu dotykowego DALI w recepcji. Dodatkowo, w sanitariatach przewidziano zastosowanie czujników obecności (CR). W pozostałych pomieszczeniach sterowanie oświetleniem odbywać się będzie miejscowo.

Oświetlenie montowane na zewnątrz budynku załączane będzie poprzez zegar sterujący lub wyłącznik zmierzchowy, z możliwością ręcznego wyłączania i włączania (dokładną lokalizację włączników ustalić na budowie).

UWAGA: Szczegóły odnośnie sterownia oświetleniem, poszczególnych scen itd. ustalić z użytkownikiem na budowie.

Wykaz dobranych opraw oświetleniowych podano na załączonej legendzie.

Ostateczny wybór opraw potwierdzić z projektantem wnętrz oraz Inwestorem.

Wysokość instalowania osprzętu (wysokości potwierdzić z projektantem wnętrz, Użytkownikiem):

– gniazdka w pokojach biurowych .....	0,3 m nad posadzką;
– gniazdka w salach .....	0,3 m nad posadzką;
– gniazdka w korytarzach .....	0,3 m nad posadzką;
– gniazdka w łazienkach .....	1,3 m nad posadzką;
– gniazdka w pom. socjalnych .....	1,1 m nad posadzką;
– łączniki .....	1,2 m nad posadzką;

## 6. INSTALACJA OŚWIETLENIA EWAKUACYJNEGO

Oświetlenie zostało zaprojektowane zgodnie z PN-EN 1838 i PN-EN 50172. Celem instalacji oświetlenia ewakuacyjnego oraz awaryjnego jest zapewnienie oświetlenia dróg ewakuacyjnych poziomym światłem o natężeniu minimum 1 lx w czasie jednej godziny od zaniku napięcia w sieci oświetlenia podstawowego, w rejonie hydrantów wewnętrznych, gaśnic oraz na klatce schodowej– 5lx.

### OPRAWY OŚWIETLENIOWE

Oświetlenie ewakuacyjne zaprojektowano lampami z własnym rezerwowym źródłem napięcia.

Przewiduje się zastosowanie opraw ściennych (jednostronnych), oraz sufitowych (dwustronnych).

Przyjęto następujące tryby pracy opraw: - oprawy awaryjne: "praca na ciemno"; - oprawy kierunkowe: "praca na jasno";

Proponuje się zastosowanie opraw ledowych o 1. godzinnym podtrzymaniu oraz z autonomicznym nadzorem.

Oprawy montować nad drzwiami oraz na ścianach, ok. 2,2 m nad posadzką.

### ZASILANIE

Zasilanie podstawowe projektowanych opraw oświetlenia ewakuacyjnego wykonać przewodami typu N2XH-J 3x1,5 z rozdzielnic RG,R1,R2,RW oraz TMPEC.

Uwaga – oprawy oświetlenia ewakuacyjnego muszą mieć odpowiedni certyfikat.

Uwaga – w przypadku stwierdzenia podczas pomiarów miejsc z niespełnieniem wymaganego natężenia oświetlenia należy instalacje rozbudować stosując dodatkowe oprawy.

## **7. INSTALACJA ZASILANIA KOMPUTEROWEGO**

Obwody zasilające odbiory komputerowe wyprowadzić z wydzielonej sekcji tablic piętrowych. Obwody należy wykonać przewodami N2XH-J / YnDYżo 3 x 2,5 układanymi w przestrzeni międzystropowej, pod tynkiem oraz pod posadzką. Każdy wypust zakończyć potrójnym gniazdkiem DATA (z blokadą dostępu). Gniazdko montować, w pobliżu gniazdek porządkowych, we wspólnych ramkach z gniazdkami logicznymi lub w puszkach podłogowych.

Dla zasilania szaf GPD oraz CCTV dobrano UPS o mocy 6kVA. UPS ma zapewnić podtrzymanie minimum 6 minut. Zasilacz UPS zasilany będzie z tablicy RS, wg schematu.

## **8. INSTALACJA SIŁY I ZASILANIA ODBIORNIKÓW TECHNOLOGICZNYCH.**

Obwody siłowe służyć będą do zasilania odbiorników technologicznych takich jak winda, urządzenia wentylacji i klimatyzacji takich jak centrale wentylacyjne, klimatyzatory itp. Zasilanie dla tych urządzeń wykonać zgodnie z wytycznymi ich producenta. Obwody zasilające poszczególne urządzenia zostały opisane na schematach ideowych.

- \* Wykonać zasilanie central wentylacyjnych (CNW...).
- \* Wykonać zasilanie nawilżacza parowego (NP).
- \* Wykonać zasilanie przepompowni (PP)
- \* Wykonać zasilanie pompy zatapialnej (PZ)
- \* Wykonać zasilanie podgrzewanych wpustów dachowych (PD)
- \* Niezależne zasilanie doprowadzić do szafy RACK (GPD oraz CCTV)
- \* Niezależne zasilanie doprowadzić do ekranów (EK...)
- \* Niezależne zasilanie doprowadzić do projektorów (PR...)
- \* Wykonać zasilanie zasilaczy (ZS)
- \* Niezależne zasilanie doprowadzić do wind (D).
- \* Niezależne zasilanie doprowadzić do podnośnika (POD).
- \* Wykonać zasilanie skrzynki rozdzielczej (R...)
- \* Wykonać zasilanie pompy (PO)
- \* Wykonać zasilanie urządzeń systemu KD oraz urządzeń systemu SSWiN
- \* Niezależne zasilanie doprowadzić do mieszarki gliny (MG)
- \* Niezależne zasilanie doprowadzić do kół gancarskich (KG)
- \* Niezależne zasilanie doprowadzić do pieców do wypalania ceramiki (PIE).
- \* Wykonać zasilanie szafki automatyki (SA)
- \* Wykonać zasilanie sterowników pomieszczeń (SP)
- \* Wykonać zasilanie urządzeń instalacji multimedialnej

\* Wykonać zasilanie klimatyzacji, jednostek wewnętrznych (KLW) i jednostki zewnętrznej (KLZ). Między jednostkami zewnętrznymi a jednostkami wewnętrznymi należy ułożyć przewody komunikacyjne, zgodnie z instrukcją producenta. Przewody komunikacyjne wykonuje firma wykonująca klimatyzację i układa je we wspólnych trasach z instalacją freonową.

Dokładne miejsce i sposób zakończenia obwodu zasilającego poszczególne odbiorniki technologiczne ustalić na budowie w porozumieniu z pracami innych branż. Wykonać zasilanie centrali sterowania oddymianiem, centrali sygnalizacji pożaru oraz zasilaczy pożarowych z przed wyłącznika pożarowego. Zasilanie urządzeń ppoż wykonać przewodami ognioodpornymi, bezhalogenowymi, np. typu NHXH PH90.

UWAGA: Przed ułożeniem zasilania do odbiorników technologicznych potwierdzić u wybranych dostawców urządzeń poprawność zabezpieczenia oraz przewodów zasilających.

## **9. INSTALACJA POŁĄCZEŃ WYRÓWNAWCZYCH**

W piwnicy, należy ułożyć szynę wyrównawczą przewodem Fe/Zn 30x4, którą należy prowadzić wzdłuż korytek kablowych, szachtach kablowych i doprowadzić do pomieszczenia wymiennikowni w której należy wykonać otok z bednarki. W okolicach rozdzielni głównej przewiduje się montaż głównej szyny wyrównawczej GSW. W pomieszczeniu serwerowni oraz wentylatorni przewiduje się montaż lokalnych szyn wyrównawczych. Do szyn należy podłączyć metalowe elementy instalacji wod-kan, co, wentylacji, korytka, szaf RACK, konstrukcje windy, ochronniki do kamer zewnętrznych obudowę i zacisk PE rozdzielnic głównej RG itp. Szynę wyrównawczą należy oznakować w żółto-zielone pasy i uziemić. Wszystkie połączenia wyrównawcze należy wykonać tak, aby nie było możliwości rozłączenia ich bez użycia narzędzi. W pomieszczeniach technicznych (serwerownia, maszynownia itp.) oraz sanitariatach wykonać miejscowe połączenia wyrównawcze przewodem H07Z1-Kżo 6 mm<sup>2</sup>(B2ca) ułożonym pod tynkiem łącząc wszystkie dostępne przewodzące części obce.

## **10. OCHRONA PRZECIWPORAŻENIOWA**

Ochronę podstawową przed dotykiem bezpośrednim stanowią będą osłony izolacyjne, bariery oraz izolacja kabli i przewodów. W celu dodatkowej ochrony przed porażeniem zaprojektowano:

- samoczynne szybkie wyłączenie zasilania w układzie TN-S dla sieci 0,4kV.

Instalacje elektryczne odbiorcze wykonane zostaną w systemie TN-S, z rozdzielonym przewodem ochronnym PE i neutralnym N w rozdzielnicach głównych 0,4kV. W celu zapewnienia dodatkowej ochrony przeciwporażeniowej w obwodach gniazd wtyczkowych, zwłaszcza w obwodach pomieszczeń narażonych na działanie wilgoci, w pomieszczeniach sanitarnych jako uzupełniający środek ochrony przed dotykiem bezpośrednim zastosowane zostaną wyłączniki ochronne różnicowo-prądowe na znamionowy prąd wyzwalający 30mA.

Metalowe obudowy opraw oświetleniowych, bolce ochronne gniazd wtykowych itp. powinny być połączone z przewodem PE. Przekrój przewodu ochronnego zgodny z PN. Wszystkie metalowe części, które mogą się znaleźć pod napięciem powinny być podłączone do systemu połączeń wyrównawczych miejscowych

## 11. OCHRONA PRZECIWPRZEPięCIOWA

W celu zabezpieczenia urządzeń elektrycznych przed skutkami przepięć indukowanych w sieci, w obiekcie przewidziano dwustopniową ochronę przed przepięciami. Ochronniki montować zgodnie ze schematami ideowymi.

## 12. INSTALACJA ODGROMOWA

Instalację wykonać zgodnie z obowiązującą normą PN-EN 62305.

Istniejącą instalację odgromową na dachu należy zdemontować, w jej miejsce projektuję się nową instalację.

Podstawową ochronę przed bezpośrednim trafieniem pioruna zapewnić mają zwody pionowe o wysokości 1,0m zainstalowane na kalenicy budynku. Szczegółowe rozmieszczenie zwodów oraz sposób ich wykonania został przedstawiony na planie instalacji odgromowej. Jako uzupełnienie ochrony zapewnianej przez zwody zainstalowane na kalenicy, w miejscach gdzie jest to konieczne należy zainstalować dodatkowe zwody pionowe. Lokalizacja tych zwodów oraz sposób ich wykonania został przedstawiony na planie instalacji odgromowej.

Zwody poziome wykonać drutem Fe/Zn  $\phi$  8 mm prowadzonych na wspornikach dachowych rozmieszczonych w odstępach nie większych niż 1m. Zwody poziome po kalenicy prowadzić na wspornikach dedykowanych.

Przewody odprowadzające wykonać drutem Fe/Zn  $\phi$  8 prowadzonym na wspornikach przykręcanych do ściany, pod tynkiem. Połączenie przewodów odprowadzających z uziomem wykonać w formie złącz kontrolnych w skrzynkach tynkowych instalowanych na wysokości 0,7m nad poziomem gruntu.

Uziom wykonać prętami uziemiającymi  $\phi$ 20, dł. 6 m. Oporność uziomu nie może przekroczyć 10 $\Omega$ . W razie potrzeby uziom należy rozbudować, wbijając kolejne pręty połączone płaskownikiem Fe/Zn30x4. Uziom układać w odległości 1m od obrysu budynku. Uziom połączyć z szyną wyrównawczą budynku. Miejsca połączeń zabezpieczyć przed korozją.

Po wykonaniu instalacji należy sporządzić i przekazać inwestorowi metrykę urządzenia odgromowego oraz protokół badań.

## 13. INSTALACJA OKABLOWANIA STRUKTURALNEGO

### Normy okablowania strukturalnego

Podstawą do przygotowania poniższego opracowania są najnowsze wydania norm okablowania strukturalnego. Wszystkie niewymienione w projekcie zagadnienia związane z okablowaniem strukturalnym są regulowane przez poniższe normy:

- **ISO/IEC 11801:2017** "Information technology. Generic cabling for customer premises".
- **EN 50173-1:2018**, "Information technology. Generic cabling systems Part 1: General requirements".
- **TIA/EIA 568.2-D:2018** "Balanced Twisted-Pair Telecommunications Cabling and Components".
- **PN-EN 50173-1:2018**, "Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne".
- **PN-EN 50174-1:2018-08**, "Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości."

- **PN-EN 50174-2:2018-08** „Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków.”
- **PN-EN 50174-3:2014-02** „Technika informatyczna. Instalacja okablowania. Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków.”
- **PN-EN 50346:2004/A2:2010** „Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania”
- **IEC 60512-99-002:2019** „Connectors for electrical and electronic equipment - Tests and measurements - Part 99-002: Endurance test schedules - Test 99b: Test schedule for unmating under electrical load”

### **Wewnętrzna kanalizacja teletechniczna**

Dla umożliwienia doprowadzenia przyłącza teletechnicznego do budynku przewidziano ułożenie dwuotworowej kanalizacji teletechnicznej do studzienki teletechnicznej na zewnątrz budynku, przy granicy działki.

Kanalizację należy wykonać z prefabrykowanych studzienek kablowych np. typu SKR-2 oraz z rur typu DVR 110 i rur RHDPE 110/6,3 pod drogami. Rury należy układać na głębokości min. 0,7m od powierzchni terenu, a pod drogami na głębokości min. 1m od nawierzchni dróg. Podaną głębokość ułożenia liczyć do górnej powierzchni kanalizacji. Rury łączyć złączkami szczelnymi. Po ułożeniu kanalizacji w połowie wysokości przykrycia ułożyć taśmę ostrzegawczą koloru pomarańczowego z odpowiednim nadrukiem.. Rury układać na podsypce piaskowej grubości 5cm, przykrywając od góry warstwą piasku grubości 10cm. Wykop należy zasypać po ułożeniu całego ciągu rur warstwami grubości do 20cm, używając ziemi z urobku i ubijać mechanicznie. Studzienkę kablową należy osadzić w wykopie w miejscu wskazanym na rysunku nr E-01. Wprowadzenia rur do studzienki kablowej i do budynków jak również same rury w budynku jak i wprowadzane kable powinny być uszczelnione gazo- i wodoszczelnie.

### **Wymagania ogólne dotyczące systemu okablowania strukturalnego**

System okablowania strukturalnego ma zapewnić niezawodną i wydajną warstwę fizyczną sieci teleinformatycznej, która zagwarantuje wystarczający zapas parametrów transmisyjnych dla działania dzisiejszych i przyszłych aplikacji transmisyjnych. W celu spełnienia najwyższych wymogów jakościowych i wydajnościowych należy zapewnić:

- Okablowanie miedziane przewyższające wymagania kategorii 6<sub>A</sub> (klasy E<sub>A</sub>).
- Okablowanie skrętkowe w wersji nieekranowanej.
- Certyfikaty wydane przez międzynarodowe, renomowane laboratorium badawcze Delta, potwierdzające zgodność okablowania miedzianego z najnowszymi, aktualnymi normami okablowania strukturalnego ISO/IEC 11801:2017, EN 50173-1:2018, TIA/EIA 568.2-D:2018. Należy zapewnić certyfikaty potwierdzające zgodność z normami w zakresie testu całego łącza oraz niezależnych komponentów (kabel, panel, złącze RJ45). Nie dopuszcza się certyfikatów z lokalnych instytutów łączności, ponieważ nie posiadają one wystarczających akredytacji do testów wszystkich parametrów wymienionych w powyższych normach.
- Wszystkie produkty muszą być fabrycznie nowe.
- Celem idealnego dopasowania komponentów, wszystkie produkty okablowania muszą pochodzić z oferty jednego producenta i być oznaczone jego nazwą lub logo.
- Należy użyć szaf 19" tego samego producenta co pozostała część okablowania strukturalnego i oznaczonych jego nazwą lub logo.
- Należy zastosować renomowany i sprawdzony w wielu instalacjach, nie tylko w Polsce, ale i w innych krajach Unii Europejskiej, system okablowania strukturalnego. Należy zastosować

przetestowany system, którego producent ma, co najmniej 15-letnie doświadczenie w produkcji okablowania strukturalnego. Zakres jego działalności w całym tym okresie musi obejmować produkcję okablowania miedzianego (kabli skrętkowych, paneli 19", złączy RJ45), światłowodowego oraz szaf dystrybucyjnych 19".

- W celu wspierania rodzimych firm z Unii Europejskiej, należy zastosować system okablowania, którego producent ma swoją główną siedzibę w jednym z krajów Unii Europejskiej.
- Producent okablowania strukturalnego musi spełniać wymagania międzynarodowej normy odnośnie standardów jakości ISO 9001, należy przedłożyć odpowiedni certyfikat.
- Producent okablowania musi objąć zainstalowany system bezpłatną, 25-letnią systemową gwarancją niezawodności, która obejmie tory transmisyjne miedziane i światłowodowe w zakresie łącza Channel (kable instalacyjne, panele 19", złącza, kable krosowe i przyłączeniowe). Gwarancja musi być trójstronną umową podpisaną pomiędzy Użytkownikiem, Wykonawcą okablowania oraz Producentem.
- Producent okablowania jest zobligowany do reasekuracji zobowiązań gwarancyjnych Wykonawcy, w przypadku niemożności wywiązania się Wykonawcy z tych zobowiązań. Reasekuracja obejmuje okres, na jaki została udzielona gwarancja.
- Warunkiem udzielenia systemowej gwarancji niezawodności jest wykonanie instalacji zgodnie z obowiązującymi normami okablowania strukturalnego oraz zgodnie z zaleceniami producenta. Instalacja musi być wykonana przez Certyfikowanego Instalatora systemu okablowania.

### **Wymagania ogólne dotyczące wykonawcy systemu okablowania strukturalnego**

Celem profesjonalnego wykonania instalacji okablowania strukturalnego, na najwyższym poziomie jakości i wydajności, wszystkich czynności instalacyjnych musi dokonać wykwalifikowana firma spełniająca poniższe wymagania:

- Firma wykonawcza musi zatrudniać pracowników – Certyfikowanych Instalatorów posiadających ważne uprawnienia i certyfikat wydany przez producenta okablowania przyjętego w tym projekcie.
- Certyfikat Instalatora musi być wydany po odbyciu szkolenia, w którym każdy Instalator zdobędzie wszystkie niezbędne umiejętności praktyczne i teoretyczne, uprawniające do instalowania, serwisowania, tworzenia dokumentacji powykonawczej oraz wykonywania pomiarów certyfikacyjnych sieci.
- Certyfikat Instalatora, który posiadają osoby wykonujące instalację musi być dokumentem terminowym wydawanym na okres jednego roku. Po tym czasie instalator musi go przedłużyć na kolejny rok, uczestnicząc w szkoleniu realizowanym przez producenta lub dystrybutora okablowania.
- Wykonawca autoryzujący system okablowania strukturalnego musi posiadać uprawnienia do objęcia zainstalowanego systemu 25-letnią systemową gwarancją niezawodności.

### **Okablowanie poziome**

Zadaniem okablowania poziomego jest zapewnienie wydajnej i niezawodnej transmisji danych pomiędzy punktami dystrybucyjnymi, a punktami przyłączeniowymi użytkowników. Długość kabla instalacyjnego, pomiędzy gniazdem RJ45 w panelu rozdzielczym a gniazdem przyłączeniowym użytkownika (nie licząc kabli krosowych i przyłączeniowych) nie powinna przekraczać 90m. Celem zapewnienia wysokiej wydajności należy zastosować okablowanie co najmniej klasy E<sub>A</sub> (kategorii 6<sub>A</sub>) wg najnowszych aktualnych standardów okablowania strukturalnego IEC61156-5, ISO/IEC11801 klasa EA, EN50173, TIA/EIA 568-C2, IEC60322-1. Zagwarantuje to odpowiedni zapas parametrów transmisyjnych dla zapewnienia transmisji danych Ethernet 10Gb/s zgodnie ze standardem IEEE 802.3bt. Zgodność z powyższymi normami należy udokumentować certyfikatami wydanymi przez niezależne laboratorium badawcze Delta w zakresie niezależnych komponentów (kabel, moduły RJ45 w panelach rozdzielczych i gniazdach przyłączeniowych).

Celem zapewnienia zasilania urządzeniom końcowym, należy zastosować komponenty okablowania strukturalnego zapewniające przesył energii zgodnie ze standardem PoEP (ang. Power over Ethernet Plus) wg IEEE 802.3at o mocy do 30W.

## Punkty przyłączeniowe użytkowników

Gniazda przyłączeniowe użytkowników (Punkty Logiczne – PL) należy zorganizować w postaci 2 modułów RJ45 keystone montowanych w adapterze z tworzywa sztucznego o wymiarach 45x45 mm. Ten uniwersalny standard montażowy zapewni organizację gniazd użytkowników w zależności od potrzeb, w formie natynkowej, podtynkowej lub w kasetach podłogowych w oparciu o osprzęt elektroinstalacyjny wielu producentów, również w połączeniu z gniazdami zasilania 230V, celem stworzenia punktów elektryczno logicznych (tzw. PEL).

W gniazdach przyłączeniowych należy zastosować moduły RJ45 keystone, które będą zapewniać:

- Kompaktowy rozmiar pozwalający na zamontowanie dwóch niezależnych modułów RJ45 keystone, w jednym uchwycie montażowym 45 x 45 mm.
- Należy zastosować komponenty o wydajności kategorii 6<sub>A</sub> (klasy E<sub>A</sub>), wg. najnowszych, aktualnych norm okablowania ISO/IEC 11801:2017, EN 50173-1:2018, TIA/EIA 568.2-D:2018. Należy to potwierdzić certyfikatem z niezależnego laboratorium badawczego (Delta lub Intertek).
- Moduł musi zapewniać wydajną transmisję w szerokim paśmie częstotliwości, dzięki wewnętrznej konstrukcji modułu keystone, w oparciu o płytkę drukowaną PCB, na której wykonane są wszystkie połączenia. Nie należy stosować modułów z wewnętrznymi połączeniami drucianymi (bez płytki PCB).
- Moduł musi zapewniać wieloletnie, niezawodne działanie, dlatego piny RJ45 muszą być pozłacane, co zagwarantuje odporność na korozję oraz łuki elektryczne powstające przy podłączaniu urządzeń PoE.
- W celu szybkiej i łatwej instalacji dla szerokiego grona instalatorów, moduły RJ45 muszą zapewniać zarówno beznarzędziowy jak i narzędziowy montaż. Sposób montażu beznarzędziowego powinien odbywać się za pomocą rozłożenia wszystkich żył kabla na „menadżerze” kabla, według naklejki określającej kolejność kolorów żył w module. „Menadżer” ten montowany jest bezpośrednio do tylnej części modułu, w której znajdują się złącza IDC. Drugi sposób montażu powinien pozwalać na zastosowanie narzędzia uderzeniowego, którym każda z żył kabla może zostać wcisnięta indywidualnie w złącze IDC. Możliwość wyboru sposobu instalacyjnego modułu daje możliwość zoptymalizowania czasu instalacji, bez względu na sposób wyszkolenia i technicznych przyzwyczajęń instalatora.
- W celu wzmocnienia i ustabilizowania kabla instalacyjnego wychodzącego ze złącza, należy zastosować moduły RJ45, w których na tylną część nakładana jest plastikowa kapsułka „menadżer”, osłaniająca złącza IDC oraz podtrzymująca kabel instalacyjny.
- Dopasowanie do płytkich puszek instalacyjnych podtynkowych i natynkowych oraz kanałów elektroinstalacyjnych, poprzez możliwość wyprowadzenia kabla instalacyjnego ze złącza na 3 sposoby, nie tylko centralnie do tyłu, ale również pod kątem 90° na lewo lub na prawo. Kątowe wyprowadzenie zapewni brak uszkodzeń kabla w wyniku przekroczenia dopuszczalnych promieni gięcia.
- Minimalizację przesłuchów międzyparowych w miejscu wprowadzania par skrętkowego kabla instalacyjnego do złącza, poprzez gwieździste rozprowadzenie par biegnących w kierunku złącza IDC. W efekcie zapewni to minimalną ilość błędów transmisyjnych. Nie należy stosować złączy, w których pary w czasie instalacji biegną równolegle w stosunku do siebie gdyż powoduje to podwyższone zakłócenia w postaci przesłuchów międzyparowych.
- Kolorową etykietę wskazującą rozprowadzenie żył skrętki w złączach IDC wg schematu T568A lub T568B. Należy zastosować schemat T568B.
- Wszystkie 8 żył skrętki musi zostać zakończonych bezpośrednio w złączu RJ45 keystone. Nie należy stosować dodatkowych rozłączalnych złączy oraz wymiennych wkładek, które stanowią dodatkowe połączenie w kanale transmisyjnych i negatywnie wpływają na parametry transmisyjne zwiększając tłumienie oraz ilość sygnałów odbitych. Wszystkie 8 pinów złącza RJ45 musi być aktywnych.
- Szeroki zakres temperatury pracy od – 40 °C do + 70 °C.
- Żywotność złącza co najmniej 1000 cykli wpięcia wtyku RJ45
- Standard mechanicznego montażu typu keystone w celu dopasowania do płyt czołowych gniazd szerokiej gamy producentów osprzętu instalacyjnego.
- Moduły tego samego typu należy zastosować w panelach rozdzielczych 19” w punktach dystrybucyjnych.
- Ilości łączy doprowadzonych do poszczególnych punktów dystrybucyjnych

## Panele rozdzielcze 19"

Przeznaczeniem paneli rozdzielczych RJ45 19" jest zakończenie skrętkowych kabli instalacyjnych, które zbiegają się do punktu dystrybucyjnego z powierzchni obiektu obsługiwanych przez dany punkt dystrybucyjny. Następnie łączy okablowania z panela rozdzielczego łączone są, przy użyciu kabli krosowych, z portami RJ45 urządzeń aktywnych lub z portami centrali telefonicznej.

W projekcie należy zastosować panele RJ45, które muszą zapewniać:

- Standardową szerokość 19" wysokość 1U oraz pojemność 24 portów RJ45 keystone (dodatkowo system okablowania użyty w projekcie musi również zawierać analogiczne panele o wysokości 2U i pojemności 48 portów, w celu zakończenia większych ilości kabli instalacyjnych).
- Montaż modułów RJ45 keystone dokładnie tego samego typu jak w gniazdach przyłączeniowych.
- Fabrycznie numerowane porty RJ45. Ułatwi to lokalizację portów w szafie 19" oraz zminimalizuje prawdopodobieństwo pomyłki przez niewłaściwe ich nazwanie.
- Łatwość montażu w stelaży 19". Należy zastosować panele szybkie w instalacji dzięki montażowi tylko na jedną śrubę M6 z każdej strony panela, umiejscowioną po środku danego U. Dodatkowo taka konstrukcja nie ogranicza dostępu do śrub montażowych (sąsiednich paneli) w porównaniu z sytuacją, gdy są one umiejscowione w narożnikach urządzenia.
- Skalowalność i pełną modułowość, umożliwiającą wypełnienie złączami RJ45 w dowolnym stopniu i dokładne dostosowanie do ilości kabli wprowadzanych do panela. Nie należy stosować paneli wykonanych w technologii płyty drukowanej PCB, w której kilka złączy trwale przytwierdzonych jest do wspólnej płytki drukowanej. Takie rozwiązanie ogranicza czynności eksploatacyjne i serwisowe, ponieważ w przypadku konieczności wymiany pojedynczego złącza RJ45 należy zdemontować i wymienić cały panel, narażając na przestój znaczącą część sieci teleinformatycznej. Rozwiązanie modułowe pozwala na serwisowanie pojedynczego złącza bez ingerencji w pozostałe tory transmisyjne.
- Łatwy dostęp do portów RJ45 w czasie krosowania dzięki umieszczeniu 24 złączy RJ45 w jednym rzędzie obok siebie. Nie należy stosować paneli, w których złącza na jednym U rozmieszczone są w kilku rządach, gdyż ogranicza to dostęp do portów, które zasłaniane są przez złącza z innych rządów, do których wpięte są kable krosowe.
- W tylnej części panela musi znajdować się prowadnica kabla, dająca możliwość trwałego przytwierdzenia skrętkowych kabli instalacyjnych, podtrzymując i zabezpieczając je przed wyrwaniem. Prowadnica ta powinna umożliwiać zamontowanie kabla instalacyjnego bez konieczności użycia dodatkowych elementów, takich jak: opaski zaciskowe lub rzepowe.
- W komplecie z panelem należy dostarczyć zestaw śrub montażowych M6.

## Skrętkowe kable instalacyjne

W celu implementacji wydajnych aplikacji, w okablowaniu poziomym przewidziano zastosowanie kabli skrętkowych Multimedia Connect nieekranowanych U/UTP kat.6<sub>A</sub> 500 MHz. Kabel skrętkowy musi zapewniać:

- Niezawodną wymianę danych dla nawet najbardziej wymagających urządzeń końcowych działających z przepływnością 10Gb/s. Należy zastosować kabel o wydajności kategorii 6<sub>A</sub> (500MHz), który spełnia wszystkie aktualne normy okablowania- IEC61156-5, ISO/IEC11801 klasa EA, EN50173, TIA/EIA 568-C2, IEC60322-1. Należy to potwierdzić certyfikatem z niezależnego laboratorium badawczego Delta, potwierdzającym przetestowanie kabla jako niezależnego komponentu pod kątem spełniania wszystkich wymienionych norm, a nie w układzie całego kanału transmisyjnego Permanent Link lub Channel.
- Zasilanie urządzeń końcowych (kamer IP, telefonów IP, punktów dostępowych WiFi itd.) wg najnowszego standardu PoEP (ang. Power over Ethernet Plus) o mocy do 30W.
- W celu minimalizacji przesłuchów obcych AlinenCrosstalk z sąsiednich łączy transmisyjnych, należy zastosować kabel o specjalnej konstrukcji minimalizującej takie zakłócenia. Należy zastosować kabel o konstrukcji spiralnej, która zapewnia najlepszą separację łączy w wiązce kabli nieekranowanych.
- W celu minimalizacji przesłuchów międzyparowych i zmniejszenia błędów w czasie transmisji, kabel musi zawierać plastikowy separator krzyżowy oddzielający sąsiednie pary. Dodatkowo

plastikowy separator zapewni większą wytrzymałość mechaniczną kabla na rozciąganie i zgniatanie oraz zapewni zachowanie bezpiecznych promieni gięcia w czasie układania.

- W celu spełnienia wymogów przeciwpożarowych należy zastosować kabel w powłoce zewnętrznej LSZH (ang. LowSmoke Zero Halogen), czyli wykonanej z materiału bezhalogenowego emitującego ograniczoną ilość szkodliwych substancji w czasie pożaru.
- Dodatkowe parametry

Parametr	Wartość
Rezystancja liniowa (maksymalna)	95 $\Omega$ / Km
Pojemność wzajemna (maksymalna)	45pF / m
Klasa CPR	B2ca s1a, d0, a1
Grubość żyły / AWG	23
Maksymalna średnica zewnętrzna	7,2 mm
Nominalna prędkość propagacji (NVP)	66 %
Temperatura pracy	- 20 °C / + 70 °C

Zgodnie z dyrektywą 305/2011 - CPR (z ang. Construction Products Regulation), która opiera się na zharmonizowanej normie europejskiej EN 50575:2014 kabel instalacyjny kategorii 6A UTP 500MHz musi posiadać klasę CPR – B2ca. Producent okablowania musi posiadać deklarację właściwości użytkowych potwierdzającą klasyfikację kabla.

### Główny punkt dystrybucyjny

Do budowy głównego punktu dystrybucyjnego należy użyć szafy 19" tego samego producenta co okablowanie strukturalne i oznaczonych tym samym logo. Należy użyć szafy serwerowej 19" 42U 800x1000 mm (szer. x gł.) o poniższych funkcjach i parametrach:

- Wytrzymała konstrukcja nawet przy pełnym wypełnieniu urządzeniami, w tym ciężkimi serwerami i UPS-ami. Szafy muszą mieć nośność co najmniej 1000 kg.
- Szafy nie mogą się chwiać pod obciążeniem, dlatego muszą mieć wzmocnione narożniki, wykonane z jednego kawałka metalu, które łączą elementy ramy szafy. Poszczególne słupy i belki ramy nie mogą być skręcane śrubami bezpośrednio z sobą, gdyż nie zapewnia to ich wystarczającej stabilności względem siebie.
- Zwiększoną nośność należy zapewnić poprzez odpowiednią grubość blachy, co najmniej 2 mm, z której wykonany jest szkielet szafy.
- Drzwi szafy nie mogą się wyginać i falować przy otwieraniu, dlatego muszą być wykonane z blachy co najmniej 2 mm grubości.
- W celu swobodnego dostępu do urządzeń zamontowanych w szafie, nawet w małych pomieszczeniach telekomunikacyjnych i pomiędzy gęsto ustawionymi rzędami szaf, szafa musi posiadać dwuskrzydłowe drzwi z przodu i tyłu, z możliwości otwarcia na 180°. Dzięki temu bez przeszkód będzie można je otworzyć nawet przy ograniczonej ilości miejsca.
- Drzwi przednie i tylne muszą zapewniać swobodny przepływ powietrza chłodzącego serwery, dlatego muszą posiadać perforację w postaci plastra miodu i przewiewnością co najmniej 80%.
- W celu zabezpieczenia urządzeń, drzwi przednie muszą posiadać zamek zamykany na klucz z trzypunktowym ryglowaniem (rygle na górze drzwi, na dole i po środku).
- W związku z częstym otwieraniem, drzwi przednie muszą posiadać metalową klamkę, która wytrzyma większą ilość cykli otwarcia w porównaniu z klamką z tworzywa sztucznego.
- Celem przeniesienia szafy nawet przez najwęższe drzwi pomieszczenia telekomunikacyjnego szafa musi posiadać możliwość rozkręcenia szkieletu, a nie tylko zdjęcia osłon.
- Belki 19" muszą posiadać regulację przód tył.
- Celem ułatwienia użytkownikowi oraz instalatorowi identyfikacji miejsca montażu urządzeń, wszystkie belki 19" muszą posiadać trwale nadrukowaną numerację jednostek U.
- Szafa musi posiadać w komplecie, zestaw linek uziemiających, dla drzwi i osłon bocznych.
- Szafa malowana proszkowo, kolor czarny, RAL 9005

W szafie PD należy przewidzieć dodatkowo montaż panela światłowodowego stanowiącego punkt styku z siecią zewnętrzną, urządzeń aktywnych, kontrolera systemu Wi-Fi oraz centrali telefonicznej.

### Specyfikacja centrali:

- **min. 9** portów abonentów wewnętrznych IP z możliwością wykorzystania funkcji provisioningu oraz obsługi BLF
- **możliwość rozbudowy** centrali o abonentów wewnętrznych systemowych i analogowych poprzez dedykowane półki tego samego producenta co centrala telefoniczna
- **możliwość wyniesienia pólek centrali** poza pomieszczenie centrali poprzez sieć LAN celem uruchomienia telefonów systemowych i analogowych w budynkach wyniesionych
- **możliwość rozbudowy** centrali do min. 300 abonentów wewnętrznych
- **min. 40** kanałów IP celem obsługi łącza miejskiego SIP trunk
- **system przygotowany do ciągłego nagrywania rozmów** z możliwością nagrywania każdego rodzaju linii miejskich oraz każdej rozmowy wewnętrznej (bez względu na port abonenta wewnętrznego) gotowy do uruchomienia jedynie poprzez zakup licencji nagrywania dla wymaganej ilości kanałów
- **system zapowiedzi słownej** dla minimum 30 kanałów rozmownych jednocześnie
- funkcja **Text2Speech**
- **system taryfikacyjny** (oprogramowanie + bufor) celem rejestracji informacji o połączeniach miejskich (przychodzących i wychodzących) zawierający także informacje o połączeniach między abonentami wewnętrznymi
- **funkcja monitorowania** pracy systemu telekomunikacyjnego z możliwością wysyłania e-mail informująca m.in. o awariach na liniach miejskich / portach wewnętrznych, wyłączeniu / przełączeniu systemu, rozładowaniu akumulatora
- programowanie systemu telekomunikacyjnego poprzez przeglądarkę internetową
- **gwarancja** na cały dostarczony sprzęt min. 24 miesiące

#### Specyfikacja telefonów:

- **1** sztuka telefonu systemowego IP tego samego producenta co system telekomunikacyjny na stanowisko sekretariatu z 5 liniowym podświetlanym wyświetlaczem, 8 programowalnymi klawiszami funkcyjnymi z diodami LED, funkcją głośnego mówienia oraz zasilaniem poprzez POE 803.2af
- **8** sztuk telefonu IP działającego w oparciu o protokół SIP, wspierającego kodek HD G.722, z 3 liniowym podświetlanym wyświetlaczem, 4 programowalnymi klawiszami funkcyjnymi z diodami LED, funkcją głośnego mówienia, wbudowanym przełącznikiem Gigabit Ethernet oraz zasilaniem poprzez POE 803.2af

#### Zalecenia i szczegółowe wymagania instalacyjne

##### Instalowanie okablowania strukturalnego

Instalację okablowania strukturalnego należy wykonać z najwyższą starannością z zachowaniem wytycznych znajdujących się w normach okablowania strukturalnego oraz wytycznych producenta okablowania. Szczególnie należy zastosować się do:

- Instalator musi zwrócić szczególną uwagę, by nie naruszyć struktury kabli podczas montażu. Należy przestrzegać bezpiecznych promieni gięcia kabli skrętkowych i światłowodowych, sił naciągu, sił zgniatających oraz przestrzegać zakresu temperatur w czasie instalacji. Dopuszczalne zakresy wymienionych parametrów można znaleźć w specyfikacjach technicznych produktów.
- Kable skrętkowe należy montować w złączach RJ45 zachowując minimalny rozplot par wprowadzanych do złącza.
- Długość skrętkowych kabli instalacyjnych pomiędzy gniazdami RJ45 w panelu rozdzielczym a gniazdami przyłączeniowymi nie może być większa niż 90m.
- Każdy moduł powinien posiadać możliwość rozszycia kabla według schematu T568A i T568B. Zaleca się stosowanie rozszycia wg schematu T568B.
- Wszystkie metalowe części szaf i stelaży dystrybucyjnych muszą zostać uziemione.
- W celu ochrony przed niepożądanym dostępem wszystkie szafy dystrybucyjne oraz pomieszczenia teletechniczne powinny zostać wyposażone w drzwi z zamkami zabezpieczającymi.
- Instalując okablowanie skrętkowe należy zachowywać poniższe bezpieczne odległości od kabli zasilających:

Typ kabla	Odległość od instalacji zasilającej [mm]		
	Brak przegrody metalicznej	Przegroda metalowa perforowana	Przegroda metalowa pełna
Kable SFTP	10	5	0
Kable UFTP; FUTP	50	25	0
Kabel UUTP	100	50	0

- ✓ Tabela obowiązuje dla wiązki 15 obwodów 230V / 20A. W przypadku mniejszej ilości obwodów, odległości proporcjonalnie się zmniejszają.
- ✓ Kable 3-fazowe należy traktować, jako 3 kable 1-fazowe.
- ✓ Obwody o prądzie większym niż 20A należy traktować, jako proporcjonalna wielokrotność obwodów 20A.
- ✓ Powyższe zalecenia obowiązują w przypadku prawidłowego uziemienia ekranów kabli transmisyjnych i metalicznych elementów tras kablowych.

### Trasy kablowe

Kable należy prowadzić w dedykowanych do tego celu trasach kablowych:

- Okablowanie w pionie między kondygnacjami należy układać w szachtach kablowych i mocować je do drabin kablowych.
- Okablowanie układane w poziomie należy instalować w korytach kablowych lub kanałach kablowych. W głównych trasach kablowych należy stosować podwieszane koryta kablowe metalowe wykonane z blachy perforowanej, które instaluje się w przestrzeni sufitowej.
- Kable skrętkowe i światłowodowe okablowania poziomego instalowane pod tynkiem należy układać w rurach osłonowych z tworzywa sztucznego. Nie należy prowadzić kabli telekomunikacyjnych i zasilających w tej samej rurze osłonowej.
- W serwerowni należy zastosować podłogę techniczną podniesioną.
- Połączenia wykonywane na zewnątrz budynków należy realizować przy wykorzystaniu dedykowanej kanalizacji teletechnicznej.

### Pomiary instalacji okablowania strukturalnego

Po wykonaniu instalacji okablowania strukturalnego wykonawca musi przeprowadzić odpowiednie pomiary sprawdzające (certyfikacyjne), wszystkich łączy miedzianych skrętkowych, potwierdzające, iż wykonane okablowanie strukturalne spełnia wymagania norm. Pomiary należy przeprowadzić zgodnie z wartościami granicznymi zdefiniowanymi w ISO 11801 lub EN 50173. Wyniki wszystkich pomiarów muszą być pozytywne. Pomiary należy wykonać przyrządem w pełni sprawnym, posiadającym ważny certyfikat potwierdzający przejście procesu kalibracji u producenta, co będzie potwierdzeniem poprawności jego wskazań. Do dokumentacji powykonawczej należy dołączyć wymieniony certyfikat kalibracji oraz raport z wynikami pomiarów wszystkich łączy okablowania skrętkowego.

### Pomiary okablowania miedzianego

Wszystkie łączy skrętkowe w systemie należy przetestować pod kątem spełniania wymogów klasy E<sub>A</sub> / kategorii 6<sub>A</sub> wg ISO 11801 lub EN 50173:

- Należy przeprowadzić pomiary w układzie pomiarowym typu „Permanent Link” (bez kabli krosowych).
- Pomiary należy wykonać miernikiem o poziomie dokładności, co najmniej „Level IV”. Zalecane typy mierników: DSX-8000, DSX-5000, DTX-1800 lub DTX-1200 firmy Fluke Networks.
- Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łączy, miernik automatycznie porówna je z granicznymi wartościami zdefiniowanymi przez aktualne normy okablowania i określi wynik porównania.
- Wyniki pomiarów certyfikacyjnych wszystkich łączy muszą być prawidłowe.
- Pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346.
- Wymagany zakres mierzonych parametrów dla każdej z par (kombinacji par):
  - ✓ Mapa połączeń - poprawność i ciągłość wykonanych połączeń

- ✓ Straty odbiciowe (ang. RL - Return Loss)
- ✓ Straty wtrąceniowe - tłumienie (ang. IL - Insertion Loss)
- ✓ Straty przesłuchów zbliżnych (ang. NEXT - Near End Crosstalk Loss)
- ✓ Sumaryczny parametr NEXT (ang. PSNEXT – Power Sum NEXT)
- ✓ Współczynnik tłumienia w odniesieniu do straty przesłuchu na bliskim końcu (ang. ACR-N – Attenuation to Crosstalk Ratio at the Near end)
- ✓ Sumaryczny współczynnik ACR-N (ang. PSACR-N – Power Sum ACR-N)
- ✓ Współczynnik tłumienia w odniesieniu do straty przesłuchu na dalekim końcu (ang. ACR-F – Attenuation to Crosstalk Ratio at the Far end)
- ✓ Sumaryczny współczynnik ACR-F (ang. PSACR-F – Power Sum ACR-F)
- ✓ Rezystancja pętli dla prądu stałego (ang. DC current loop)
- ✓ Opóźnienie propagacji (ang. Propagation delay)
- ✓ Różnica opóźnień propagacji (ang. Delay skew)

### **Pomiary instalacji okablowania strukturalnego**

Po wykonaniu instalacji okablowania strukturalnego wykonawca musi przeprowadzić odpowiednie pomiary sprawdzające (certyfikacyjne), wszystkich łączy miedzianych skrętkowych, potwierdzające, iż wykonane okablowanie strukturalne spełnia wymagania norm. Pomiary należy przeprowadzić zgodnie z wartościami granicznymi zdefiniowanymi w ISO 11801 lub EN 50173. Wyniki wszystkich pomiarów muszą być pozytywne. Pomiary należy wykonać przyrządem w pełni sprawnym, posiadającym ważny certyfikat potwierdzający przejście procesu kalibracji u producenta, co będzie potwierdzeniem poprawności jego wskazań. Do dokumentacji powykonawczej należy dołączyć wymieniony certyfikat kalibracji oraz raport z wynikami pomiarów wszystkich łączy okablowania skrętkowego.

### **Pomiary okablowania światłowodowego**

Wszystkie łączy światłowodowe w systemie należy przetestować pod kątem spełniania wymogów norm ISO 11801 lub EN 50173:

- Należy przeprowadzić pomiary dwukierunkowe, w których źródło świetlnego sygnału referencyjnego będzie umieszczone w pierwszym kroku na jednym końcu łączy, a w kolejnym kroku na drugim końcu łączy.
- Łączy wielomodowe (MM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 850 nm i 1300 nm.
- Łączy jednomodowe (SM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 1310 nm i 1550 nm.
- Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łączy, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania.
- Wyniki pomiarów certyfikacyjnych wszystkich łączy muszą być prawidłowe.
- Pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346.
- Wymagany zakres mierzonych parametrów:
  - ✓ Ciągłość łączy.
  - ✓ Długość łączy.
  - ✓ Tłumienie włókien dla dwóch długości fali.

### **Dokumentacja powykonawcza**

Po wykonaniu instalacji wykonawca jest zobowiązany do sporządzenia dokumentacji powykonawczej, która będzie zawierała:

- Opis instalacji, przedstawiający architekturę systemu oraz charakterystykę rozwiązań technicznych zastosowanych w systemie okablowania.
- Listę produktów, z ilościami, wykorzystanych do budowy sieci okablowania strukturalnego.
- Schemat oznaczeń łączy miedzianych i światłowodowych.
- Podkłady budowlane z zaznaczeniem: łączy, punktów przyłączeniowych użytkowników oraz punktów dystrybucyjnych.
- Schemat blokowy instalacji.
- Rysunki przedstawiające wyposażenie punktów dystrybucyjnych.
- Pozytywne wyniki pomiarów wszystkich łączy wg normy EN 50173 lub ISO/IEC 11801.
- Certyfikat potwierdzający ważność kalibracji przyrządu, którym wykonano pomiary

Dokumentację należy sporządzić w dwóch kopiach: jedna przeznaczona dla Inwestora, druga przeznaczona dla producenta, celem uzyskania gwarancji systemowej.

### Wymagania gwarancyjne

Inwestor oczekuje, że zainstalowany system okablowania strukturalnego będzie działał niezawodnie przez wiele lat. Dlatego wymagane jest udzielenie przez Producenta 25-letniej systemowej, bezpłatnej gwarancji niezawodności, która zapewni:

- Zgodność ze standardami okablowania strukturalnego obowiązującymi w czasie wykonania instalacji.
- Niezawodne działanie aplikacji (protokołów transmisyjnych), zdefiniowanych w standardach okablowania strukturalnego obowiązujących w czasie wykonania instalacji, dla których system został zaprojektowany.
- Brak wad fabrycznych elementów łączy okablowania oraz błędów w czasie instalacji okablowania.

W tym celu w ciągu 30 dni od daty zakończenia instalacji Wykonawca powinien zgłosić Producentowi potrzebę udzielenia gwarancji i dostarczyć wymaganą dokumentację powykonawczą oraz pomiary sieci okablowania strukturalnego. W ciągu kolejnych 15 dni Wykonawca jest zobowiązany do dostarczenia Inwestorowi certyfikatu gwarancyjnego łącznie ze szczegółowymi warunkami gwarancyjnymi, z uwzględnieniem wymagań zawartych w dokumentacji powyżej.

Przykładowe zestawienie podstawowych materiałów:

Lp.	Nazwa produktu	Jedn.	Ilość	Uwagi
1	<b>Szafa GPD</b>			
2	Szafa serwerowa, 42U, 800x1000x1995mm, podwójne, perforowane drzwi z przodu i z tyłu	szt.	1	
3	Cokół do szafy dystrybucyjnej 800x1000mm, wysokość 100mm	szt.	1	
4	Panel wentylacyjny 4-wentylatorowy z termostatem	szt.	1	
5	Listwa zasilająca 19" 9x230V	szt.	1	
6	Panel porządkujący 19"/1U	szt.	9	
7	Panel 19" 1U z gniazdami 6xLC dx, 12 pigtaili, SM	szt.	1	przylącz zewnętrzny
8	Panel 24xRJ45 BC 1U, bez modułów	szt.	8	
9	Moduł RJ45 BC kat.6A UTP TL	szt.	192	
10	Patch. kat. 6A U/UTP LSZH 1m LINK+, szary	szt.	165	
11	Przełącznik 24 x GE PoE+ + 4 GE SFP Web Smart Pro Switch, PoE Budget max.200W, 1 RJ45 Console port	szt.	1	dla Wi-Fi
12	Przełącznik 24 x GE PoE+ + 4 GE SFP Web Smart Pro Switch, PoE Budget max.200W, 1 RJ45 Console port	szt.	1	dla telefoni VoIP
13	Przełącznik Web Smart Pro Switch, supports 48 x GE ports + 4 x integrated Gigabit SFP ports. SFP ports can be used for redundant links.	szt.	3	dla LAN
14	<b>Gniazda</b>			
15	Moduł RJ45 BC kat.6A UTP TL	szt.	165	
16	Gniazdo 45x45 mm dla 1xRJ45 BC, podtyinkowe, bez modułów RJ45 (komplet: ramka, support, puszka, adapter)	szt.	13	
17	Gniazdo 45x45mm dla 2xRJ45 BC, podtyinkowe, bez modułów RJ45 (komplet: ramka, support, puszka, adapter)	szt.	76	
18	Patch. kat. 6A U/UTP LSZH 1m LINK+, szary	szt.	14	podłączenie Access Pointów
19	Patch. kat. 6A U/UTP LSZH 3m LINK+, szary	szt.	122	użytkownicy
20	<b>Kable instalacyjne</b>			
21	Kabel U/UTP kat.6A 500 MHz LSZH B2ca	m	Wg rzutów	
22	<b>System Wi-Fi</b>			
23	Sprzętowy kontroler Wi-Fi, obsługa do 50 Access Pointów, zawiera licencje na AP	szt.	1	

24	Indoor Access Point, 802.11 a/b/g/n/ac ; Wave 2; Concurrent Dual-band 2.4 / 5 GHz, DC Input: 12V / 1.0A, PoE: 802.3af compliant (PoE injector optional), Uplink: 1 x 10/100/1000Base-T Ethernet, Auto MDIX, RJ-45 with 802.3af PoE, LAN: 1 x 10/100/1000Base-T Ethernet, Auto MDIX, RJ-45, USB: 1 x USB 2.0 Port	szt.	14	
25	<b>Centrala telefoniczna wg specyfikacji</b>	Kpl.	1	
26	telefonu systemowego IP tego samego producenta co system telekomunikacyjny stanowisko sekretariatu z 5 liniowym podświetlanym wyświetlaczem, 8 programowalnymi klawiszami funkcyjnymi z diodami LED, funkcją głośnego mówienia oraz zasilaniem poprzez POE 803.2af	Szt.	1	
27	telefonu IP działającego w oparciu o protokół SIP, wspierającego kodek HD G.722, z 3 liniowym podświetlanym wyświetlaczem, 4 programowalnymi klawiszami funkcyjnymi z diodami LED, funkcją głośnego mówienia, wbudowanym przełącznikiem Gigabit Ethernet oraz zasilaniem poprzez POE 803.2af	Szt.	8	

#### 14. INSTALACJA SYGNALIZACJI POŻARU.

Instalację sygnalizacji pożaru zaprojektowano w oparciu o interaktywny, adresowalny system sygnalizacji pożarowej, który automatycznie wykrywa miejsce powstania pożaru i włącza urządzenie sygnalizacyjne i wykonawcze oraz zapisuje w pamięci zaistniałe zdarzenia. Wszystkie urządzenia wchodzące w skład systemu muszą spełniać wymagania norm serii EN-54 i posiadają wymagane w Polsce atesty. Projekt opracowano w oparciu o podstawowe zasady projektowania instalacji sygnalizacji pożarowej CNBOP.

Podstawowe urządzenia systemu to:

#### CENTRALKA SYSTEMU SYGNALIZACJI POŻARU

##### Parametry Centrali Sygnalizacji Pożarowej:

- **Świadectwo dopuszczenia CNBOP jako centrala sygnalizacji pożarowej oraz zasilacz urządzeń przeciwpożarowych**
- Modułowa budowa umożliwia łatwą rozbudowę,
- Graficzny, kolorowy, 7-calowy panel dotykowy
- 4x interfejs Ethernet
- Możliwość rozbudowy od 1 do 4 pętli
- Możliwość wymiany poszczególnych modułów funkcjonalnych bez konieczności wyłączania całego systemu oraz ponownego programowania centrali po wymianie modułów,
- Możliwość dowolnego umieszczania modułów w slotach (zabudowana elektronika we wszystkich modułach funkcjonalnych, brak możliwości dostępu do elementów elektroniki modułów zapewnia zwiększoną odporność mechaniczną i elektrostatyczną),
- Linie dozoru mogą pracować w układzie pętli, linii otwartej, odgałęzienia ( T-Tap)
- Pętle dozoru mogą być prowadzone kablem ekranowanym i nieekranowanym
- Maksymalna ilość elementów na pętli 254
- Możliwość stworzenia 4096 stref dozoru,
- Możliwość integracji kilku języków w panelu obsługi centrali
- Możliwość zapewnienia pętli dozoru o długości 3000 m lub prądzie 1,5A,
- Możliwość podłączenia certyfikowanego wyniesionego panelu obsługi (potwierdzone ważnym Świadectwem Dopuszczenia)
- Możliwość stworzenia 5000 grup logicznych
- Możliwość stworzenia 128 zestawów logicznych
- Pamięć zdarzeń 10000
- Możliwość przyłączenia systemów wizualizacji po protokole komunikacyjnym OPC Serwer i RS232

**Centrala ponadto powinna:**

- pracować w systemie adresowalnym tzn. umożliwiać identyfikację numeru i rodzaju elementu zainstalowanego w pętli dozorowej,
- mieć wbudowaną pamięć zdarzeń i alarmów,
- mieć duży, czytelny, dotykowy wyświetlacz LCD umożliwiający uzyskanie pełnej informacji, dotyczącej stanu systemu oraz ułatwiający konfigurację i obsługę centrali,
- umożliwić podłączenie adresowalnych elementów liniowych, służących do sterowania i kontroli urządzeń dodatkowych, współpracujących z systemem p.poż,
- umożliwić podłączenie adresowalnych elementów liniowych z odgałęzieniami bocznymi dla czujek konwencjonalnych,
- umożliwić blokowanie alarmów pochodzących od elementów liniowych na określony czas lub na stałe,
- współpracować z urządzeniami monitoringu pożarowego,
- posiadać modułową architekturę, by dobrze dostosować możliwości centrali do potrzeb obiektu,
- umożliwić sterowanie urządzeniami przeciwpożarowymi za pomocą wyjść przekaźnikowych.
- umożliwić grupowanie sterowań urządzeniami przeciwpożarowymi,
- umożliwić synchroniczne wystawianie do kilkudziesięciu wyjść sterujących jednocześnie,
- umożliwić podłączenie do 127 elementów adresowalnych na jednej linii dozorowej,
- umożliwić wykonanie testowania lub blokowania elementów oraz przygotowanie odpowiedniego raportu,
- umożliwić podłączenia systemu komputerowego w celu przedstawienia stanu systemu w formie graficznej na ekranie monitora,

CENTRALKA SYGNALIZACJI POŻARU POWINNA BYĆ PODŁĄCZONA DO SYSTEMU MONITOROWANIA STRAŻY POŻARNEJ.

**ELEMENTY OSTRZEGAWCZE**

Jako elementy ostrzegawcze współpracujące z centralką sygnalizacji pożaru przewidziano:

**CZUJKI POŻAROWE**

Główną cechą charakterystyczną czujek jest bardzo duża dokładność i szybkość wykrywania zagrożenia - szczególnie czujki z dwoma detektorami, które są w stanie wykryć już niewielkie zadymienie.

**Podstawowe funkcje**

W zależności od rodzaju czujki, czujki posiadają odpowiednie detektory, które można konfigurować przy pomocy timera i sieci lub ręcznie. Praca odbywa się w sposób ciągły – sygnały analizowane są przez układy elektroniczne znajdujące się wewnątrz czujki, po czym łączone są przez wbudowany mikroprocesor. Zastosowanie różnych detektorów w jednej czujce zwiększa odporność na fałszywe alarmy, mimo oddziaływania na nią wielu czynników, tj. kurz, para, dym. Dzięki możliwości odpowiedniego zaprogramowania, alarm włączy się tylko w danej konfiguracji. Opcja ta gwarantuje dużą niezawodność, jak również zapobiega przed zbyt dużą ilością fałszywych alarmów. Dodatkowo

analizowany jest także czas sygnałów pożaru i sygnał usterek. W przypadku detektorów optycznego i chemicznego istnieje możliwość określenia progu wyzwolenia alarmu przez ich regulację.

#### **Detektor optyczny (dymu)**

Detektor optyczny działa na zasadzie pomiaru rozproszenia światła. W przypadku zadymienia, dym unosząc się do góry przenika do komory pomiarowej, gdzie następuje rozproszenie światła emitowanego przez diodę LED. W zależności od ilości światła, powstaje odpowiedni sygnał elektryczny. Czujki posiadające dwa detektory optyczne działają na zasadzie różnic w długości fali. Cechą unikalną jest zastosowanie technologii Dual Ray, która wykorzystując światło podczerwone i niebieski diod LED umożliwia wykryć nawet niewielkie zadymienie (TF1 i TF9).

#### **Detektor termiczny (temperatury)**

Głównym elementem tego rodzaju czujek jest termistor posiadający konwerter analogowo – cyfrowy, który prowadzi pomiar napięcia zależnego od temperatury w równych odstępach czasu. Wyróżniamy dwa rodzaje czujek:

- czujki nadmiarowe – uruchamiają się po przekroczeniu określonej temperatury 54°C lub 69°C,
- czujki różnicowe – uruchamiają się przy zarejestrowaniu wzrostu temperatury w określonym przedziale czasu

#### **Pozostałe właściwości**

- wyzwolenie alarmu widoczne jest dzięki migającej w kolorze czerwonym diodzie LED w zakresie 360°
  - istnieje możliwość podłączenia czujek do wyniesionego wskaźnika zadziałania,
  - łatwy dostęp do zacisków
  - odporność na kurz konstrukcji układu optycznego i pokrywy,
  - możliwość czyszczenia czujek przy użyciu sprężonego powietrza, dzięki znajdującemu się w pokrywie specjalnemu otworowi,
  - nie ma konieczności regulacji położenia podstawy czujki, dzięki centralnemu położeniu diod alarmowych,
  - posiadają blokadę uniemożliwiającą wyjęcie czujki z podstawy.

### **CZUJKI ZASYSAJĄCE**

Zasysające czujki dymu zostały zaprojektowane specjalnie pod kątem bezpośredniej współpracy z lokalną siecią bezpieczeństwa o rozbudowanej funkcjonalności. Są to aktywne układy detekcji pożaru, służące do wczesnego wykrywania pożaru w monitorowanym obszarze oraz do monitorowania urządzeń, kanałów wentylacyjnych i klimatyzacyjnych. Wykorzystują one najnowszą technologię detekcji. Odporność na zanieczyszczenia, kompensacja temperaturowa sygnałów pochodzących z detektorów oraz uruchamianie z uwzględnieniem ciśnienia powietrza gwarantują niezawodne działanie nawet w najbardziej niesprzyjających parametrach środowiskowych.

#### **Zasada działania**

Urządzenie zasysające pobiera próbki powietrza z monitorowanego obszaru przez układ rurek ze zdefiniowanymi otworami próbkującymi i przekazuje pobrane próbki do modułu czujki. W zależności od czułości reakcji modułu czujki, zasysająca czujka dymu wyzwala alarm w momencie wykrycia określonego poziomu gęstości dymu. Alarm jest sygnalizowany za pomocą diody LED w urządzeniu i

przesyłany do centrali sygnalizacji pożaru. Detektor przepływu powietrza wykrywa pęknięcia lub niedrożności rurek zasysających.

Funkcja inteligentnego przetwarzania sygnału porównuje mierzony poziom zadymienia ze znanymi zmiennymi zakłócającymi i na tej podstawie określa wiarygodność alarmu. Można ustawić różne czasy opóźnienia wyświetlania i przesyłania alarmu. Wszystkie moduły czujek są monitorowane pod kątem zanieczyszczenia, awarii lub usunięcia urządzenia.

Komunikat o awarii można zresetować z poziomu centrali sygnalizacji pożaru. Połączenie przez lokalną sieć bezpieczeństwa zapewnia równoczesne resetowanie alarmów i komunikatów o usterce w urządzeniu i w linii dozоровej.

Do zasysających czujek dymu dostępne są trzy różne moduły czujek. Moduły te posiadają różne czułości reakcji:

Maks. czułość (osłabienie promieniowania świetlnego)	Poziomy
0,5%/m (0,8%/m)	2
0,1%/m (0,25%/m)	4
0,015%/m (0,05%/m)	4

#### Rozmieszczenie czujek

Układ rurek wraz z otworami próbkującymi został zaprojektowany i musi być wykonany symetrycznie (odchylenie  $\pm 10\%$ ). Jeśli uwarunkowania strukturalne uniemożliwiają zachowanie żądanej symetrii, należy przestrzegać następujących zasad:

- liczba otworów próbkujących powietrze i długość najkrótszego oraz najdłuższego odgałęzienia rurki w układzie rurek zasysających nie może przekraczać stosunku 1:2.
- odległość między sąsiednimi otworami próbkującymi w rurce zasysającej musi być równa (maks. odchylenie  $\pm 20\%$ ).
- średnice otworów próbkujących określa się osobno dla każdego odgałęzienia rurki. Średnice zależą od łącznej liczby otworów w danym odgałęzieniu rurki.

Systemy przewodów zasysających są konstruowane zgodnie ze specyfikacjami dotyczącymi planowania, obejmującymi typowe elementy przewodów rurowych oraz elementy do zastosowań specjalnych np. rozdzielacz wody lub bariera przeciwwybuchowa.

Wszystkie otwory w systemach zasysania dymu mają średnicę 1 cm, a dokładne średnice otworów są ustalane za pomocą opatentowanych foliowych kryz redukcji zasysania. Do każdego otworu zasysającego musi być dostarczona foliowa kryza redukcji zasysania z odpowiednią średnicą otworu oraz taśma znakująca.

Dobór i rozmieszczenie układu rur i otworów zasysających został sprawdzony przy wykorzystaniu oprogramowania producenta na zgodność z wymaganiami normy EN54-20.

#### Podłączenie do pętli dozоровej

Czujki zasysające podłączane są bezpośrednio do sieci bezpieczeństwa, dzięki czemu oferują wszystkie zalety technologii. Dane robocze i komunikaty o usterce są widoczne na kontrolerze centrali. Po wystąpieniu alarmu do centrali sygnalizacji pożaru przesyłane są dane identyfikacyjne poszczególnych czujek.

Do zasilania czujek przewidziane zostały buforowe zasilacze pożarowe, nadzorowane przez pętlowe moduły wejść pod kątem poprawności działania.

#### Parametry techniczne:

- Napięcie pracy 15 VDC - 33 VDC

- Pobór prądu z sieci 6,25 mA
- Pobór prądu z zasilacza dodatkowego (przy napięciu 24 V)
  - prąd rozruchu, napięcie zasilania wentylatora 6,9 V 300 mA
  - pąd rozruchu, napięcie zasilania wentylatora 9 V 300 mA
  - w trybie czuwania, napięcie zasilania wentylatora 6,9 V 200 mA
  - w trybie czuwania, napięcie zasilania wentylatora 9 V 260 mA
  - w trybie alarmowym, napięcie zasilania wentylatora 6,9 V 230 mA
  - w trybie alarmowym, napięcie zasilania wentylatora 9 V 290 mA
- Stopień ochrony zgodnie z normą EN 60529 IP 20
- Dopuszczalny zakres temperatur
  - zasysające czujki dymu -20°C ÷ +60°C
  - układ rurek zasysających z tworzywa PVC 00°C ÷ +60°C
  - układ rurek zasysających z tworzywa ABS -40°C ÷ +80°C
- Dopuszczalna wilgotność względna (bez kondensacji) 10 - 95%
- Czułość reakcji (maks. osłabienie promieniowania)
  - Moduł czujki 0,5%/m (0,8%/m)
  - Moduł czujki 0,1%/m (0,25%/m)
  - Moduł czujki 0,015%/m (0,05%/m)
- Żywotność wentylatora (12 V) 43 000 godz. przy 24°C

### MODUŁ M1: 8-wejściowy moduł interfejsu z wyjściem przekaźnikowym

#### PODSTAWOWE WŁAŚCIWOŚCI:

- Monitorowanie maksymalnie ośmiu wejść
- Zestyk przełączny, umożliwiający beznapięciowy styk wyjściowy
- Monitorowanie zestyków impulsem 8mA – stan pracy „zwarty” lub „rozarty”
- Monitorowanie linii przy pomocy rezystora końcowego 3,9kΩ (czuwani3, przerwa w linii, zwarcie)
- Maks. prąd obciążenia: 2A/30VDC lub 0,5A/42,4VAC
- Wbudowany obustronny izolator zwarć zgodny z normą EN54-17
- Zasilanie z linii dozorowej
- Przełączniki obrotowe umożliwiają adresowanie ręczne lub automatyczne
- Zgodny z normą EN54-18
- Podkładki dystansowe umożliwiają montaż na nierównej powierzchni

<b>Napięcie wejściowe:</b>	15-33 VDC
<b>Maks. pobór prądu</b>	5,5 mA
<b>Wartości rezystancji linii:</b>	tryb czuwania: 1500-6000 mΩ; przerwa: >12000 mΩ; zwarcie: <800 mΩ
<b>Monitorowanie zestyków – prąd maksymalny:</b>	8 mA
<b>Tryb pracy przekaźnika:</b>	NC/COM, COM/NO
<b>Maks. obciążenie styków przekaźnika:</b>	2A/30VDC; 0,5A/42,4VAC
<b>Min. prąd przełączania:</b>	0,01 mA
<b>Dopuszczalny przekrój żył:</b>	0,6-3,3 mm <sup>2</sup>
<b>Temp. pracy:</b>	-20 - +65 °C
<b>Klasa ochrony</b>	IP54

### MODUŁ M2: Moduł 8 wyjść przekaźników niskonapięciowych

#### PODSTAWOWE WŁAŚCIWOŚCI:

- Zestyk przełączny, umożliwiający beznapięciowy styk wyjściowy
- Możliwość dołączenia maks. 8 elementów zewnętrznych
- Maks. obciążalność styków: 2A/30VDC
- Wbudowany obustronny izolator zwarć zgodny z normą EN54-17
- Zasilanie z linii dozorowej
- Przełączniki obrotowe umożliwiają adresowanie ręczne lub automatyczne
- Praca w trybie NO/COM/NC
- Zgodny z normą EN54-18
- Podkładki dystansowe umożliwiają montaż na nierównej powierzchni

<b>Napięcie wejściowe:</b>	15-33 VDC
----------------------------	-----------

<b>Maks. pobór prądu</b>	3,55 mA
<b>Monitorowanie zestyków – prąd maksymalny:</b>	8 mA
<b>Tryb pracy przekaźnika:</b>	NC/COM/NO
<b>Min. prąd przełączania:</b>	0,01 mA/ 10mVDC
<b>Dopuszczalny przekrój żył:</b>	0,6-3,3 mm <sup>2</sup>
<b>Temp. pracy:</b>	-20 - +65 °C
<b>Klasa ochrony</b>	IP54

#### **MODUŁ M5: Moduł przekaźników wysokiego napięcia**

##### **PODSTAWOWE WŁAŚCIWOŚCI:**

- Dwa przekaźniki maks. 230VAC
- Możliwość sterowania wentylatorem dzięki funkcji FAN
- Przełączniki obrotowe umożliwiają adresowanie ręczne lub automatyczne
- Panel LED wyświetlający stan pracy
- Zasilanie z linii dozоровej
- Wbudowany obustronny izolator zwarć zgodny z normą EN54-17
- Dostępny z obudową do montażu natynkowego lub na szynie DIN
- Zestyki zabezpieczone bezpiecznikami 10A
- Możliwość stosowania kabli nieekranowanych
- Zgodny z normą EN54-18

<b>Napięcie wejściowe:</b>	15 VDC – 33VDC
<b>Maks. pobór prądu:</b>	17,15 mA
<b>Maks. obciążenie styków:</b>	10 A (przy napięciu 24VDC, 120VAC, 230VAC), 6 A (przy napięciu 30VDC)
<b>Maks. napięcie sygnału zwrotnego:</b>	30VDC
<b>Maks. czas zwłoki styku NC:</b>	9 ms
<b>Temp. pracy:</b>	-20 - +50°C
<b>Klasa ochrony:</b>	IP54 (moduł w obudowie), IP30 (moduł na szynę DIN)

#### **MODUŁ M6: Moduł 1 wyjść przekaźników niskonapięciowych**

##### **PODSTAWOWE WŁAŚCIWOŚCI:**

- Zestyk przełączny, umożliwiający beznapięciowy styk wyjściowy
- Wbudowany obustronny izolator zwarć zgodny z normą EN54-17
- Zasilanie z linii dozоровej
- Przełączniki obrotowe umożliwiają adresowanie ręczne lub automatyczne
- Praca w trybie NO/COM/NC
- Zgodny z normą EN54-18
- Podkładki dystansowe umożliwiają montaż na nierównej powierzchni
- możliwość montażu na szynie DIN bądź w obudowie natynkowej

<b>Napięcie wejściowe:</b>	15-33 VDC
<b>Maks. pobór prądu</b>	1,75 mA
<b>Max. prąd przełączania:</b>	5A
<b>Tryb pracy przekaźnika:</b>	NC/COM/NO
<b>Min. prąd przełączania:</b>	0,1 mA/ 100mVDC
<b>Dopuszczalny przekrój żył:</b>	0,6-3,3 mm <sup>2</sup>
<b>Temp. pracy:</b>	-20 - +55 °C
<b>Klasa ochrony</b>	IP30

#### **Sygnalizator wewnętrzny biały**

##### **Cechy:**

- Zgodny z EN54-3
- W celu lepszej ochrony ludzi akustyczny alarm nie powinien być przerywany w przypadku awarii pętli spowodowanej przerwą w linii, zwarcie lub zwarcie doziemnym. Ma to również

zastosowanie, gdy sygnalizator jest zainstalowany w odgałęzieniu lub gdy kabel pętli jest zniszczony po obu stronach.

- Możliwe jest zamontowanie ponad 50 sygnalizatorów tego typu w jednej pętli
- Poziom ciśnienia akustycznego nie zmniejsza się, gdy spada napięcie (od 33 V do 20 V)
- Głośność można regulować z panelu sterowania wykrywaniem pożaru w 5 krokach.
- Monitorowane sterowanie i zasilanie napięciem przez system magistrali pierścieniowej
- Adresowanie interfejsu automatycznie lub za pomocą przełącznika kodu (umożliwiającego unikalne przyporządkowanie lokalizacji instalacji do adresu)
- 2 izolatory (jeden dla linii wejściowej i jeden dla linii wychodzącej) zintegrowane z czujnikiem w celu utrzymania operacyjnej dostępności wszystkich elementów w pętli, nawet w przypadku zwarcia, dlatego kable o wytrzymałości funkcjonalnej nie są wymagane. Izolatory są zgodne z EN54-17
- Można użyć nieekranowanego kabla

Parametry elektryczne		
Napięcie pracy		15-33VDC
Pobór prądu:	Tryb czuwania Alarm	<1mA
		=<4,35mA
Parametry środowiskowe		
Temperatura pracy		-10 do +55°C
Inne		
Maksymalny poziom ciśnienia akustycznego w odl. 1m		101,3 dB(A)
Zakres częstotliwości		440Hz – 2,9 kHz
Źródło zasilania		
Typ		3V, litowa
Pojemność		2,6Ah
Typowa żywotność		>10 lat
Dopuszczalna temp. pracy		-25 do +70°C
Stopień ochrony		IP21 C (IP42*)

## WPC: Klawiatura wyniesiona

Klawiatura wyniesiona umożliwia prawidłowy i estetyczny montaż w widocznych miejscach. Umożliwia montaż pod kątem oraz natynkowy i podtynkowy bez konieczności samodzielnego montażu ram montażowych.

Sieć łączy klawiatury wyniesione z centralami sygnalizacji pożaru.

Klawiatura wyniesiona umożliwia zdecentralizowaną pracę całego systemu ochrony przeciwpożarowej. Wygląd graficznego interfejsu użytkownika jest taki sam jak na centrali sygnalizacji pożaru. Centrale i klawiatury mogą wyświetlać wszystkie komunikaty i działać jako jeden zdecentralizowany system. Dodatkowo możliwe jest tworzenie oddzielnych grup. W ramach jednej grupy wyświetlane i obsługiwane są tylko komunikaty o opcje sterowania central w danej grupie.

## Sygnalizowanie alarmu

Aby obsługiwać system ekran dotykowy powinien być dostępny na klawiaturze wyniesionej. Wyświetlacz musi mieć wielkość co najmniej 7" (po przekątnej) i minimalną rozdzielczość 800 x 480 pikseli. Podświetlenie zapewnia wyraźną czytelność ekranu. Graficzny interfejs użytkownika jest łatwy

w obsłudze i można go dostosowywać do różnych sytuacji. Umożliwia to prawidłową obsługę, która jest prosta i intuicyjna. Wyświetlacz pokazuje wszystkie komunikaty w jasnym, wyróżniającym się kolorze. Wyświetlane komunikaty zawierają następujące informacje:

- typ komunikatu/wiadomości
- typ elementu wyzwalającego
- jednoznaczny opis złożony z co najmniej 32 znaków zawierający dokładną lokalizację elementu wyzwalającego
- strefa logiczna i adres podrzędny elementu wyzwalającego

Każde nowe zdarzenie uruchamia sygnał akustyczny o natężeniu co najmniej 65 dB wytwarzany przez brzęczyk zintegrowany z klawiaturą wyniesioną. Operator musi mieć możliwość wyciszenia sygnału za pomocą określonego przycisku na klawiaturze.

Diody LED stanu zapewniają jasne informacje na temat stanu całego systemu. Jednoznaczne symbole oświetlone kolorowymi diodami LED wskazują stan określonych urządzeń. Ikony LED odzwierciedlają następujące typy urządzeń:

- czujki alarmu pożarowego
- urządzenia sygnalizacyjne
- urządzenia transmisyjne
- urządzenia ochrony przeciwpożarowej
- zasilania

Określony kolor wskazuje następujące stany:

- czerwony: stan alarmu pożarowego
- żółty: stan usterki lub funkcja wyłączona
- zielony: stan gotowości, urządzenie dostępne

Weryfikacja alarmu

Operator może weryfikować przychodzące komunikaty alarmowe o pożarze za pomocą klawiatury wyniesionej, aby uniknąć przypadkowego uruchomienia urządzeń sygnalizacyjnych i przeciwpożarowych w wyniku niewłaściwego użycia. System może działać w dwóch trybach: nocnym i dziennym. Interfejs użytkownika jednoznacznie wskazuje, który z tych dwóch trybów jest aktualnie używany. Operator z odpowiednimi uprawnieniami może przełączać się między trybami dziennym i nocnym.

Przegląd stref ewakuacyjnych i wyjść

Operator może w dowolnym momencie uzyskać informacje o wszystkich strefach alarmowych i wyjściach podłączonych do urządzeń przeciwpożarowych. Każda strefa i każde wyjście jest oznaczone wyraźnym opisem złożonym z co najmniej 30 znaków zawierającym dokładny opis

lokalizacji. Wyróżniający się kolor (czerwony, żółty, zielony) wskazuje stan poszczególnych stref i wyjść. Operator z odpowiednimi uprawnieniami może ręcznie rozpocząć ewakuację w wybranych strefach i aktywować wyjścia podłączone do urządzeń przeciwpożarowych.

### Funkcje operatora

Za pomocą klawiatury wyniesionej operator może wykonywać określone funkcje zarządzania całym systemem sygnalizacji pożaru. Za pośrednictwem graficznego interfejsu użytkownika operator ma dostęp co najmniej do następujących funkcji:

- resetowanie 1 czujki, strefy czujek lub całego systemu;
- wyciszanie wbudowanego brzęczyka;
- wyciszanie urządzeń sygnalizacyjnych;
- przełączanie między trybem dziennym i nocnym;
- wyłączanie czujek, urządzeń sygnalizujących i wyjść;
- odczyt rejestru historii;
- uruchamianie sprawdzenia lub obchodów testowych przez jedną osobę;
- ustawianie daty i godziny;
- regulacja czułości automatycznych czujek pożarowych;
- regulacja schematu wykrywania wielu kryteriów czujek pożarowych;

Klawiatura wyniesiona jest wyposażona w co najmniej trzy programowalne klawisze funkcyjne. Za pomocą tych klawiszy funkcyjnych operator może łatwo aktywować określone często używane funkcje. Każdy klawisz funkcyjny ma wskaźnik stanu, który jest aktywny podczas wykonywania funkcji. W dowolnym momencie operator mający odpowiednie uprawnienia może sterować klawiszami funkcyjnymi.

### Zapisywanie komunikatów

Klawiatura wyniesiona zapisuje wszystkie przychodzące alarmy i zdarzenia w dzienniku historii.

Dziennik historii jest przechowywany w pamięci flash mieszczącej co najmniej 10 000 wiadomości. W przypadku całkowitego odłączenia zasilania zdarzenia pozostają zapisane w pamięci. Każde zdarzenie jest zapisywane z następującymi informacjami:

- unikatowy numer sekwencji
- typ komunikatu/wiadomości
- data i godzina zdarzenia
- jednoznaczny opis złożony z co najmniej 32 znaków zawierający dokładną lokalizację elementu wyzwalającego
- strefa logiczna i adres podrzędny elementu wyzwalającego

Operator może przeglądać dziennik historii w porządku chronologicznym za pośrednictwem graficznego interfejsu użytkownika centrali. Przy użyciu filtra można wyszukiwać poszczególne zdarzenia, przedziały czasowe lub urządzenia peryferyjne.

Można eksportować dziennik historii do pliku \*.PDF lub \*.CSV.

## Języki

Operator może zmienić język graficznego interfejsu użytkownika. Język jest bezpośrednio dostosowywany do wyboru użytkownika bez ponownego uruchamiania centrali sygnalizacji pożaru. Integrator przekazuje użytkownikowi wydrukowaną skróconą instrukcję obsługi w ramach odbioru systemu. Dostępne są następujące języki: angielski, bułgarski, chorwacki, czeski, duński, estoński, francuski, grecki, hebrajski, hiszpański, holenderski, litewski, łotewski, niemiecki, polski, portugalski, rosyjski, rumuński, serbski, słowacki, słoweński, szwedzki, turecki, ukraiński, węgierski i włoski. Integrator przekazuje użytkownikowi wydrukowaną skróconą instrukcję obsługi w ramach odbioru systemu.

## Przełącznik Ethernet

Klawiatura wyniesiona ma wbudowaną kartę sieciową z co najmniej czterema portami zewnętrznymi. Porty te mogą obsługiwać szybkość transmisji do 100 Mb/s. Przełącznik Ethernet stosuje się do interfejsów danych w następujących instalacjach:

- sieć central
- system automatyki budynkowej
- system integrujący
- serwer usługi zdalnej

W przypadku kabla miedzianego jego maksymalna długość wynosi 100 m. Opcjonalnie dzięki zastosowaniu konwerterów transmisji do kabla światłowodowego odległość tę można wydłużyć do 40 km.

## Zasilanie sieciowe i zasilanie zapasowe

Aby zagwarantować integralność funkcjonalną, klawiatura wyniesiona ma dwa wejścia zasilania. Klawiatura jest zasilana z centrali sygnalizacji pożaru oraz zasilacza zewnętrznego. O ile jest to możliwe, używane główne źródło zasilania. Gdy zasilacz główny ulegnie awarii, jego funkcję może przejąć zasilacz redundantny. W przypadku odcięcia zasilania lub błędów klawiatura generuje komunikat o usterce.

Klawiatura wyniosła jest zgodna z normą: EN 54-2:1997 + A1:2006

#### Parametry techniczne

- Parametry elektryczne
  - Zakres napięcia wejściowego: 13,2–30 V DC
- Parametry mechaniczne
  - Wskaźnik palności: UL94-V0
  - Materiał obudowy: poliwęglan
  - Kolor: RAL9003, biały sygnałowy. Lakierowana
- Parametry środowiskowe
  - Dopuszczalna temperatura otoczenia podczas pracy: -5°C do 50°C
  - Dopuszczalna temperatura przechowywania: -20°C do 60°C
  - Wilgotność względna: do 95% bez kondensacji przy 25°C
  - Stopień ochrony: IP 30

#### Tryby pracy systemu sygnalizacji pożarowej

W zależności od zaprogramowania system może być przystosowany do jednego lub dwóch trybów pracy, czyli do trybu nocnego lub trybu dziennego i nocnego. Jeśli system przystosowano do trybu pracy dziennej i nocnej, przełączanie trybów może odbywać się automatycznie przez sterowanie czasowe lub za pomocą przycisku.

##### Tryb Nocny:

- Każdy z alarmów pochodzący z czujek jest od razu traktowany jako ALARM II STOPNIA. Całkowicie automatycznie odbywa się wystawienie wszystkich urządzeń przeciwpożarowych, zgodnie z zaprogramowanym algorytmem działania.

##### Tryb Dzienny:

- W trybie pracy dziennej niezbędna jest obecność przeszkolonego oraz dostępnego w trakcie czasu opóźnienia personelu obsługi;
- Po zadziałaniu elementu liniowego w adresowalnej linii dozorowej centrala, na podstawie algorytmów decyzyjnych, sygnalizuje ALARM I STOPNIA lub ALARM II STOPNIA w zależności od wariantów alarmowania zaprogramowanych dla konkretnych stref. Po wystąpieniu alarmu I stopnia (pobudzenie czujki) system pracujący w trybie dziennym przechodzi w tzw. układ interwencji.

Alarm I Stopnia jest alarmem wewnętrznym i wymaga zawsze zgłoszenia się personelu i potwierdzenia alarmu przyciskiem „ROZPOZNANIE” - w czasie T1 oraz rozpoznania zagrożenia w obiekcie w czasie T2. W czasie T2 jest możliwość skasowania alarmu przyciskiem „KASOWANIE”, jeśli obsługa uzna, że nie ma zagrożenia. Do tego momentu centrala sygnalizuje alarm I stopnia. Podczas, gdy obsługa ma czas na rozpoznanie naciśnięcie któregośkolwiek ROP'a wywołuje od razu alarm II stopnia. Jeśli brak jest reakcji personelu na alarm I stopnia, wówczas jest wywoływany alarm II stopnia.

Alarm II stopnia jest wewnętrznym stanem centrali, który powoduje, oprócz wywołania w centrali sygnalizacji optycznej, przekazanie sygnału o pożarze.

Wystąpienie w centrali alarmu II stopnia powoduje automatyczne przejście stref będących w alarmie I stopnia w stan alarmu II stopnia.

Alarm II stopnia może być poprzedzony alarmem I stopnia lub jest generowany natychmiastowo w zależności od zaprogramowanego wariantu alarmowania dla konkretnej strefy w obiekcie lub trybu pracy centrali. Alarm II stopnia jest wezwaniem do natychmiastowego podjęcia akcji gaśniczej.

Resetowanie centrali odbywa się po naciśnięciu przycisku „Kasowanie Alarmu”.

Uruchomienie ręcznego ostrzegacza pożarowego wywołuje od razu „ALARM II STOPNIA”.

### **Montaż instalacji i prowadzenie okablowania systemu sygnalizacji pożarowej**

Montaż wykonywać zgodnie z obowiązującymi w kraju normami i przepisami.

Celem uniknięcia kolizji zaleca się przeprowadzenie montażu instalacji systemu sygnalizacji pożarowej po wykonaniu innych instalacji w obiekcie lub koordynować ich wykonanie na bieżąco z innymi branżami. Połączenia pętli dozorowych wykonać kablami HTKSHekw PH90 1x2x0. Połączenie pętli sterujących HTKSHekw PH90 1x2x0,8. Obwód linii zasilającej centralę wykonać kablem NHXH-J PH90 3x2,5 PH90 3x2,5mm<sup>2</sup> (opracowanie w części elektrycznej).

Pozostałe okablowanie zgodnie ze schematem ideowym. Sposób układania przyjąć taki sam jak dla instalacji elektrycznych zachowując zgodność z certyfikatem kabla.

W razie wykrycia pomieszczenia, w którym nie przewidziano czujki należy skontaktować się z Projektantem instalacji lub osobą pełniącą nadzór autorski w celu uzupełnienia czujek.

Moduły pętlowe instalować w miejscach umożliwiających przegląd i konserwację.

W przypadkach kolizji lub zbliżeń zachować odległość 50cm czujek od ścian, podciągów, przewodów wentylacyjnych.

Zachować odległość czujek min. 1,5m od kratki wentylacyjnych nawiewu i wywiewu.

Czujki w celach należy zabezpieczyć indywidualna konstrukcja siatki w celu zabezpieczenia przed demontażem.

Zachować odległość min. 30cm przewodów instalacji SSP od innych przewodów i kabli elektrycznych.

Początki i końce linii dozorowych prowadzone w częściach pionowych instalacji prowadzić w osobnych rurach, przy czym dopuszcza się stosowanie wspólnej rury dla „początków” i końców linii pętlowej.

Ręczne ostrzegacze pożaru instalować na wysokości 1,2-1,6 m od podłogi.

Centralę sygnalizacji pożaru zainstalować na wysokości umożliwiającej swobodny odczyt informacji z jej pola odczytowego.

Wszystkie zmiany powstałe podczas montażu instalacji należy nanieść w dokumentacji powykonawczej.

### **KONSERWACJA I UTRZYMANIE SYSTEMU**

Na podstawie specyfikacji technicznej nr PKN CEN/TS 54-14 poniżej przedstawiono warunki eksploatacji systemu SSP. Wymagania te określają ramowy i szczegółowy zakres prac konserwacyjnych oraz obsługi technicznej.

### **Obsługa codzienna:**

Użytkownik powinien zapewnić, aby codziennie było sprawdzane:

- Czy panel centrali wskazuje stan dozoru, lub czy każde odchylenie od stanu dozoru jest odnotowane w książce pracy.
- Czy przy każdym alarmie zarejestrowanym od poprzedniego dnia podjęto odpowiednie działania.
- Każda zauważona nieprawidłowość powinna być odnotowana w książce pracy i możliwie szybko usunięta.

### **Obsługa miesięczna:**

Co najmniej raz w miesiącu użytkownik powinien zapewnić aby:

- Zapasy papieru, tuszu lub taśmy dla każdej drukarki były wystarczające.
- Przeprowadzono test wskaźników a każdy fakt niesprawności wskaźnika został odnotowany.
- Każda zauważona nieprawidłowość powinna być odnotowana w książce pracy i możliwie szybko usunięta.

### **Obsługa kwartalna:**

Co najmniej jeden raz na każde 3 miesiące, użytkownik powinien zapewnić, aby specjalista sprawdził wszystkie zapisy w książce pracy i podjął niezbędne działania, aby doprowadzić do prawidłowej pracy instalacji.

- Spowodować zadziałanie, co najmniej jednej czujki lub ręcznego ostrzegacza pożarowego w każdej strefie, w celu sprawdzenia czy centrala prawidłowo odbiera i wyświetla określone sygnały, emituje alarm akustyczny oraz uruchamia wszystkie inne urządzenia ostrzegawcze i pomocnicze.
- Dokonać rozpoznania, czy w budynku nastąpiły jakieś zmiany budowlane lub w jego przeznaczeniu, które mogłyby wpłynąć na rozmieszczenie czujek i ręcznych ostrzegaczy pożarowych oraz sygnalizatorów akustycznych.

### **Obsługa roczna:**

Co najmniej jeden raz w roku, użytkownik powinien zapewnić, aby specjalista przeprowadził próby zalecane dla obsługi codziennej, miesięcznej i kwartalnej.

- Sprawdzić każdą czujkę na poprawność działania zgodnie z zaleceniami producenta. Chociaż każda czujka powinna być sprawdzana raz w roku, dopuszcza się sprawdzanie kolejnych 25% czujek przy kolejnej kontroli kwartalnej.
- Sprawdzić zdolność centrali sygnalizacji pożarowej do uaktywnienia wszystkich funkcji pomocniczych.
- Sprawdzić wzrokowo, czy wszystkie połączenia kablowe i sprzęt są sprawne, nieuszkodzone i odpowiednio zabezpieczone.
- Dokonać oględzin, czy w budynku nastąpiły jakieś zmiany budowlane lub w jego przeznaczeniu, które mogłyby wpłynąć na rozmieszczenie czujek i ręcznych ostrzegaczy pożarowych oraz sygnalizatorów akustycznych. Oględziny powinny także potwierdzić, czy

pod każdą czujką jest utrzymana wolna przestrzeń co najmniej 0,5 m we wszystkich kierunkach i czy wszystkie ręczne ostrzegacze pożarowe są dostępne i widoczne.

- Sprawdzić i przeprowadzić próby wszystkich baterii akumulatorów.
- Każda zauważona nieprawidłowość powinna być odnotowana w książce pracy i możliwie szybko usunięta.

#### Dokumentacja:

Po zakończeniu przeglądu kwartalnego i rocznego, jednostka odpowiedzialna, za przeprowadzenie próby powinna dostarczyć osobie odpowiedzialnej, z potwierdzeniem odbioru, protokół stwierdzający, że próby wymienione w instrukcji zostały wykonane i, że o wykrytych wadach została powiadomiona osoba odpowiedzialna.

#### Dobór akumulatorów:

Nazwa	Rozmiar aku.	Pojemność aku., Ah	Czas podtrzymania...	Czas alarm., min	Całkowity prąd w tryb...	Całkowity prąd alarm...	Całkowita wymagana...	Wymagane aku.	Wymagane moduły kontrolera aku.
1 wartość(s)	1 wartość(s)	1 wartość(s)	1 wartość(s)	1 wartość(s)	1 wartość(s)	1 wartość(s)	1 wartość(s)	1 wartość(s)	1 wartość(s)
Centrala 1	Duży, 36-45 Ah	40	72	30	641,3	1028,5	46687,9	4	1

#### ZESTAWIENIE PODSTAWOWYCH MATERIAŁÓW:

Lp.	Opis	Ilość
1.	Centrala z kontrolerem w wersji premium, montaż na ramie	1
2.	Klawiatura wyniesiona	1
3.	Obudowa zasilania średnia do instalacji czterech baterii 12V/40Ah oraz jednego uchwytu zasilacza pojedynczego (cena obejmuje uchwyt zasilacza pojedynczy)	1
4.	Rama montażowa średnia	1
5.	Zestaw kabli połączeniowych (moduł BCM/baterie - 180 cm; bateria/bateria - 17cm) Wykorzystywane, gdy baterie są umieszczone w oddzielnej obudowie)	2
6.	Zestaw kabli połączeniowych pomiędzy modułem BCM a zasilaczem UPS (długość 150 cm)	1
7.	Akumulator 40Ah/12V	4
8.	Moduł pętli o obciążalności 300mA	1
9.	Moduł 8 wyjść przekaźnikowych niskonapięciowych	1
10.	Czujka optyczna Dual Ray z przełącznikami obrotowymi	57
11.	Czujka optyczno-termiczna Dual Ray z przełącznikami obrotowymi	2
12.	Gniazdo czujek	59
13.	Wskaźnik zadziałania	21
14.	ROP czerwony, wewnętrzny	12
15.	Klucz do Ręcznego Ostrzegacza Pożarowego - 5 sztuk	3
16.	Zapasowa szybka do Ręcznych OstrzeGaczy Pożarowych - 5 sztuk	3
17.	Adresowalny sygnalizator akustyczny z baterią, wewnętrzny, biały	19
18.	Moduł 8 wejści 1 wyjścia przekaźnikowego niskonapięciowego wraz z obudową	8
19.	Moduł 8 wyjść przekaźnikowych niskonapięciowych wraz z obudową	1
20.	Moduł wyjść przekaźnikowych wysokonapięciowych 2 wyjścia/2 wejścia , z obudową	3
21.	Moduł wyjść przekaźnikowych niskonapięciowych (1 przekaźnik), montaż szyna DIN	1
22.	Obudowa do modułów	1
23.	Zasysająca czujka dymu z panelem wskaźników LED, sygnalizujących tryb pracy, usterkę i alarm	1
24.	Podstawa obudowy do zasysającej czujki dymu	1
25.	Filtr duże pudełko	1
26.	Folia redukcyjna X.X mm (cena za 1szt)	3
27.	Taśmy znakujące AF-BR do kryz redukcji zasysania	3

28.	Rura PCV 25mm szara [m]	20
29.	Zatyczka do rur 25mm PCV szara	1
30.	Kolanko 90 stopni do rurek 25mm z PCV łuk -szare	3
31.	Uchwyt do rur 25/27mm bezhalogenowy szary	10
32.	Złączka do rur 25mm z PCV Mufa-szara	20
33.	PVC-U Klej UNI-100 1000ml	1
34.	PVC-U Zmywacz 1000ml	1
35.	Zasilacz 27,6V/3A/2x28Ah zasilacz do systemów przeciwpożarowych 1,8A/27,6VDC - dla pracy ciągłej – I <sub>max</sub> a; 3,0A/27,6VDC - dla pracy chwilowej – I <sub>max</sub> b (5min) IBAT=1,2A; 2x28Ah; 420 x 407 x 178+8	2
36.	Zasilacz 27,6V/5A/2x17Ah zasilacz buforowy impulsowy Grade 2, 5A/27,6VDC; IBAT=1A/2A; 2x17Ah; 330 x 380 x 173+14,	1
37.	Zasilacz 27,6V/10A/2x40Ah zasilacz buforowy impulsowy Grade 2, 10A/27,6VDC; IBAT=1A/2A/4A; 2x40Ah; 460 x 390 x 173+14	2
38.	Akumulator 12V/18Ah	2
39.	Akumulator 12V/28Ah	4
40.	Akumulator 12V/40Ah	4

## 15. INSTALACJA STEROWANIA ODDYMIANIEM KL. SCHODOWYCH

Kłapy oddymiające klatkę schodową będą otwierać się automatycznie, razem z drzwiami napowietrzającymi. Układ sterujący składa się z centrali oddymiania (COD), przycisków alarmowych oraz siłowników. Dodatkowo przewiduje się zastosowanie przycisku przewietrzania, umożliwiającego otwieranie i zamykanie klapy na życzenie, oraz montowanej na dachu stacji pogodowej. System oddymiania należy zintegrować z instalacją sygnalizacji pożaru.

Okablowanie instalacji sterowania oddymianiem grawitacyjnym

W instalacji sterowania oddymianiem grawitacyjnym wykorzystane zostaną następujące typy okablowania:

- podłączenia siłowników do centrali oddymiania - HDGs PH90 3x2,5mm<sup>2</sup>,
- podłączenia przycisków oddymiających do centrali oddymiania – HTKSH PH90 4x2x0,8mm,
- podłączenie przycisków przewietrzających do centrali oddymiania – HTKSHekw 4x2x0,8mm,
- podłączenie centrali pogodowej do centrali oddymiania – N2XH-J 3x1,5,
- podłączenie czujek dymu do centrali oddymiania – HTKSHekw 1x2x0,8mm
- podłączenie modułu SSP do centrali oddymiania – okablowanie i moduł w zakresie opracowania instalacji SSP.

Należy stosować jedynie okablowanie zgodne z najnowszą dyrektywą CPR oraz normą SEP N SEP-E-007:2017-09

Montaż urządzeń

Dokładne rozmieszczenie urządzeń zostało pokazane na rzutach. Przewody należy instalować tak, aby chronić je przed uszkodzeniami. Przewody prowadzić wydzieloną trasą z zachowaniem odstępu od przewodów elektrycznych. Przewody należy prowadzić w rurkach ochronnych bezhalogenowych montowanych w bruzdach pod tynkiem. Kable pożarowe montować za pomocą dedykowanych uchwytów w bruzdach pod tynkiem.

Montaż wszystkich urządzeń wykonać zgodnie z DTR poszczególnych urządzeń oraz według wytycznych producenta.

Przejścia przewodów instalacji przez ściany zewnętrzne oraz wewnętrzne pomiędzy strefami pożarowymi uszczelnić przy pomocy mas uszczelniających o odporności właściwej dla ścian, które są uszczelniane. Przyciski montować na wysokości 1,2-1,6m.

Zalecenia uruchamiania, eksploatacji i konserwacji

Przed przekazaniem systemu do eksploatacji zaleca się dokładne sprawdzenie systemu i przeprowadzenie prób funkcjonalnych oraz przeprowadzenie pomiarów sprawdzających wszystkich łączy. Należy również wykonać dokumentację powykonawczą oraz przeszkolić pracowników obsługujących system.

ZESTAWIENIE PODSTAWOWYCH MATERIAŁÓW:

Opis	ilość
<b>Centrale oddymiania</b>	
zasilacz z centralą oddymiania 16A (2x8A), 1 linia-2 grupy, 315x305x160mm, 2x9Ah	1
akumulator bezobsługowy, wykonany w technologii, 152x100x64mm, konektor 4,8mm	2
<b>Elementy systemu</b>	
czujka dymu optyczna	3
podstawa czujki	3
ręczny przycisk oddymiania z sygnalizacją optyczno-akustyczną, natynkowy, kolor pomarańczowy, obudowa IP30, 6 żył, współpraca z centralą oddymiania   CNBOP	3
przycisk przewietrzania klawiaturowy z sygnalizacją diodową, natynkowy, 24VDC, współpraca z centralą oddymiania	1
czujka pogodowa deszcz-wiatr	1

## 16. SYSTEM ZARZĄDZANIA INSTALACJAMI BEZPIECZEŃSTWA - SMS

W celu zintegrowania wszystkich systemów bezpieczeństwa w ramach obiektu planuje się połączyć poszczególne podsystemy jednym wspólnym oprogramowaniem zarządzania bezpieczeństwem.

Oprogramowanie integrujące Security Management System (SMS) pozwoli zarządzać systemami z pozycji jednego wspólnego interfejsu, zapewniając pełną automatyzację i integrację obsługi procesów związanych z bezpieczeństwem obiektu.

Zakłada się budowę systemu modułowego i skalowalnego w pełnej architekturze klient – serwer, komunikującego się z podsystemami poprzez interfejs OPC. Architektura systemu pozwala na współpracę

z różnymi sieciami LAN/WAN przy użyciu standardowego sprzętu i oprogramowania.

Systemy podlegające integracji w ramach platformy:

- CCTV
- SSWiN
- SSP
- KD

Funkcjonalności oprogramowania integrującego

Wszystkie istotne systemy bezpieczeństwa obiektowego zbudowane zostaną w oparciu o sieć TCP/IP. Sieć komputerowa jest więc naturalna platforma do integracji SMS. Zakłada się instalację

serwera zarządzania bezpieczeństwem wyposażonego w dedykowane oprogramowanie zapewniające następujące funkcje użytkowe:

- praca w architekturze klient-serwer
- komunikacja z urządzeniami poprzez interfejs OPC
- 128-bitowe szyfrowanie pomiędzy serwerem a stacjami operatorskimi
- przechowywanie zdarzeń ze wszystkich systemów w jednej zunifikowanej bazie danych SQL
- możliwość automatycznego wykonywania zaprogramowanych scenariuszy postępowania w zależności od rodzaju zdarzenia
  - baza danych zabezpieczona przed ingerencją osób nieuprawnionych
  - interfejs użytkownika bazujący na serwerze sieciowym ze stronami HTML
  - automatyczne rozpoznanie rozdzielczości monitora i uruchamianie interfejsu z odpowiednimi ustawieniami
  - wykorzystanie w pełni skalowalnych map wektorowych (np. AutoCad) do wizualizacji każdego rozmiaru obiektu
  - możliwość pracy w standardowej infrastrukturze LAN/WAN
  - możliwość budowy scenariuszy działania systemu w zależności od zdarzenia
  - nadzorowanie statusów wszystkich elementów systemu
  - sterowanie elementami systemu (np. zazbrajanie / rozbrajanie stref systemu SSWiN)
  - zapewnienie bezpiecznego połączenia z serwerem za pomocą SSL
  - obsługa oprogramowania w języku polskim
  - prezentowanie liczników zdarzeń, oddzielnie dla zdarzeń wszystkich kategorii. Musi istnieć możliwość filtrowania widoku zdarzeń na liście (stosie) alarmów na zdarzenia wybranej kategorii poprzez prostą operację (np. kliknięcie). Umożliwianie ustawienia kolejności wyświetlania zdarzeń alarmowych przynajmniej według (lp., czasu, identyfikatora czujnika, zdarzenia, priorytetu, kategorii) rosnąco lub malejąco
  - zdarzenia muszą być prezentowane na liście zdarzeń w jednowierszowej postaci zwartej. Musi istnieć możliwość edycji postaci zwartej – wymagana jest możliwość wyboru wyświetlanych danych spośród: lp. czas i data, nazwa (lokalizacja), zdarzenia, stan obecny, priorytet, kategoria, status, użytkownik
  - umożliwianie zdalnego sterowania elementami systemu na mapie wektorowej (np.: blokowanie drzwi, otwieranie drzwi na stałe, otwieranie drzwi, sterowanie kamerami PTZ, zazbrajanie i rozbrajanie stref SSWiN itp.)
  - wspomaganie użytkownika w podejmowanych działaniach za pośrednictwem procedur postępowania operatora, zróżnicowanych w zależności od rodzaju i kategorii zdarzenia (np. graficzne instrukcje potwierdzania alarmu włamania)
  - możliwość definiowania użytkowników z podziałem na grupy funkcjonalne z przypisaniem do nich poziomów uprawnień
  - możliwość definiowania użytkowników z możliwością przydzielania uprawnień wg np.: integrowanych systemów, wykonywanych określonych akcji

- bieżące rejestrowanie wszystkich zdarzeń systemowych (dziennik zdarzeń), w tym odbierane komunikaty i podejmowane działania
  - możliwość definiowania i generowania raportów ze zdarzeń w obiekcie także w oparciu o harmonogramy czasowe (np. raporty dzienne, miesięczne, kwartalne itp)
  - nadzorowanie połączeń systemów integrowanych (np.: SSWiN, CCTV, SSP, KD)
  - możliwość wykonywania backupu online całego serwera (pełny oraz przyrostowy/zgodny z harmonogramem) oraz odtwarzania z wcześniejszych kopii
  - możliwość wykonywania backupu online konfiguracji serwera i backupu bazy danych serwera oraz odtwarzania z wcześniejszych kopii
  - wymagana jest możliwość skonfigurowania systemu z wieloma stanowiskami roboczymi, w tym ze zdalnymi lokalizacjami (np. za pośrednictwem przeglądarki internetowej z zachowaniem pełnej funkcjonalności systemu)
  - niezakłócona praca wszystkich systemów zintegrowanych nawet w przypadku ewentualnego wyłączenia / awarii platformy
  - dowolna liczba operatorów systemu z indywidualnie przydzielonymi uprawnieniami
- Konfiguracja systemu SMS powinna pozwolić na obsługę nie mniej niż:
- 10 000 kontrolowanych punktów detekcyjnych
  - Nielimitowaną liczbą jednocześnie podłączonych podsystemów
  - Nielimitowaną liczbą stacji roboczych
  - Nielimitowaną liczbą zdarzeń/alarmów
  - 1000 alarmów obsługiwanych w kolejce

W zakresie integracji poszczególnych podsystemów bezpieczeństwa zakłada się poniższe właściwości funkcjonalne.

#### **Integracja z CCTV:**

- wizualizacja lokalizacji kamer na mapach obiektowych wspólnie z pozostałymi powiązanymi systemami
- pełna integracja z oprogramowaniem VMS
- przekazywanie alarmów podsystemów bezpieczeństwa do systemu VMS celem wyświetlania obrazów powiązanych kamer
- obsługa zdarzeń alarmowych systemu CCTV w systemie integrującym (sabotaż kamery, zanik wideo, naruszenie strefy inteligentnej analizy obrazu itp.)
- nadzorowanie statusów wszystkich elementów systemu

#### **Integracja z Systemem Kontroli Dostępu:**

- wizualizacja na żywo wszystkich przejść przez punkty kontroli dostępu
- konfiguracja systemu Kontroli Dostępu
- zarządzanie użytkownikami (np. dodawanie, usuwanie, blokowanie, edytowanie)
- zarządzanie prawami dostępu (np. tworzenie profili dostępu, przydzielania praw użytkownikom)
- nadzorowanie statusów wszystkich elementów systemu
- sterowanie elementami systemu (np. blokowanie drzwi, otwieranie drzwi na stałe,
- możliwość zautomatyzowania uzbrajania/rozbrajania stref

- modele czasowe do kontroli dostępu zdefiniowane na poszczególne dni tygodnia łącznie z konfiguracjami obejmującymi dni wolne, święta itp.
- modele czasowe automatycznego uaktywniania / blokowania ustawień karty, np. zasad dostępu, kodów PIN itp.
- modele czasowe automatycznego uaktywniania / blokowania ustawień systemowych, np. stałego otwarcia drzwi od godziny 9 do 17
  - czasowe uaktywnienie/blokowanie karty, ręczne lub zgodne z ustalonym harmonogramem
  - kontrola kolejności przejścia (anti-passback)
  - obchód wartowniczy wykorzystujący istniejące czytniki kontroli dostępu, kolejność dostępu oraz kontrolę czasu dostępu.
- funkcja trasy wymuszająca na użytkownikach poruszanie się na określonych trasach wewnątrz obiektu
- możliwość ograniczania maksymalnej liczby osób które mogą znajdować się w danym obszarze logicznym
- zarządzanie alarmami w szerokim zakresie warunków ich uruchamiania, np. w wyniku odmowy dostępu, alarmu sabotażu, użycia niedozwolonego identyfikatora, alarmu pod przymusem, itd., które może zostać uzupełnione ogólnie dostępnymi funkcjami SMS, takimi jak wyświetlanie map lokalizacji i planów działania
- eksport danych do standardowego formatu CSV w celu dalszej obróbki

#### **Integracja z Systemem SSWiN:**

- wizualizacja na mapie stanu czujek oraz stref
- możliwość uzbrajania/rozbrajania czujek/stref
- możliwość odbierania alarmów w przypadku naruszenia stref uzbrojonych
- nadzorowanie statusów wszystkich elementów systemu

#### **Integracja z Systemem SSP:**

- wizualizacja na mapie stanu czujek oraz stref
- możliwość odbierania alarmów
- nadzorowanie statusów wszystkich elementów systemu

#### **Obsługa operatorska:**

Podstawowym polem do obsługi systemu SMS będzie wysokowydajna stacja operatorska. W zakresie określonych potrzeb system wizualizowany będzie na monitorze w formie podkładów obiektowych

z naniesionymi elementami poszczególnych systemów bezpieczeństwa. Najważniejsze cechy interfejsu do wizualizacji to:

- Wizualizacja stanów wszystkich elementów (detektorów) podsystemów w oparciu o mapy wektorowe (płynna możliwość zbliżania, oddalania, poruszania się po mapie)
- czujniki na planie wyświetlane warstwowo dla poszczególnych systemów, z możliwością wygaszania warstw i zdefiniowanych widoków (wycinków) na wypadek zdarzenia z danego systemu
- zapewnienie zdalnego sterowania elementami systemu na mapie wektorowej (np.: blokowanie drzwi, otwieranie drzwi na stałe, otwieranie drzwi, zazbrajanie i rozbrajanie stref systemu SSWiN, itp.)

- wizualizacja powiązań pomiędzy systemami (np.; prezentacja obrazu z kamery umieszczonej w strefie zadziałania czujnika detekcji ruchu lub pożaru)
- możliwość uruchomienia funkcji wideo weryfikacji zdarzeń kontroli dostępu (tzn. po przyłożeniu karty do czytnika przez użytkownika, operatorowi wyświetli się obraz bieżący z kamery w przejściu wraz ze zdjęciem użytkownika z systemu. Otwarcie drzwi zostanie wyzwolone przez operatora SMS po weryfikacji tożsamości)
- wyświetlanie alarmów w sposób graficzny
- złożony hierarchiczny system uprawnień operatorów w zakresie otrzymywanych informacji i ich wyświetlania na ekranie oraz dostępu do poszczególnych części aplikacji
- nadzorowanie połączeń z systemami podłączonymi do niego
- automatyczne wykonywanie zaprogramowanych scenariuszy postępowania w zależności od rodzaju zdarzenia
- możliwość dostosowania interfejsu użytkownika oraz tworzenia spersonalizowanych komunikatów systemowych (np. dołożenie dodatkowych przycisków funkcyjnych w interfejsie bądź pól na wpisanie raportu w komunikacie)
- zapewnienie bezpiecznego połączenia z serwerem za pomocą SSL
- obsługa oprogramowania w języku polskim

Zestawienie podstawowych materiałów:

Lp.	Opis	Ilość
1.	Wysokiej wydajności serwer z procesorem Intel Xeon Silver 4208 (2,1 GHz, 8-core, 11 MB, 85 W), pamięć RDIMM 32 GB (2 x 16 GB) CAS-19-19-19 (DDR4-2666), 4-portowa karta Ethernet 1GB, do szafy rack 19", wysokość 2U	1
2.	Stacja robocza Z4G4 - wysoka wydajność (z kartą NVIDIA Quadro P2200)	1
3.	Przemysłowy monitor LED wysokiej rozdzielczości dedykowany do rozwiązań HD, 32", 1920 x 1080px, Wejścia HDMI, DVI, VGA, DisplayPort, czas reakcji 8 ms	2
4.	Pakiet podstawowy	1
5.	Automation Engine - Pakiet podstawowy	1
6.	1 000 dodatkowych punktów detekcyjnych	1
7.	Integracja	1
8.	Access Engine - Pakiet podstawowy	1

## 17. INSTALACJA KONTROLI DOSTĘPU

W budynku, dla wybranych pomieszczeń przewiduje się wykonanie instalacji systemu kontroli dostępu (KD). W drzwiach objętych systemem kontroli dostępu zostaną zainstalowane zamki elektromagnetyczne, czytniki zbliżeniowe umożliwiające otwarcie drzwi za pomocą karty oraz przyciski umożliwiające awaryjne otwarcie drzwi w przypadku ewakuacji. W ościeżnicach drzwi zainstalowane zostaną kontaktrony do sygnalizacji i rejestracji otwarcia drzwi.

### Opis ogólny systemu

#### SYSTEM KONTROLI DOSTĘPU

1. System kontroli dostępu umożliwia sterowanie drzwiami za pomocą czytnika karty zbliżeniowej oraz stacji roboczej systemu kontroli dostępu

2. Czytnik karty zbliżeniowej zawiera także klawiaturę numeryczną używaną, jeśli wymagany jest dostęp za pomocą karty i kodu PIN
3. System kontroli dostępu powinien spełniać wymogi GRADE 3
4. System kontroli dostępu powinien obsługiwać również szlabany oraz windy do 56 pięter
5. Utrata komunikacji pomiędzy oprogramowaniem zarządzającym a kontrolerami nie powinna mieć wpływu na normalne działanie systemu.
6. System kontroli dostępu jest zaprojektowany w taki sposób, aby awaria dowolnego kontrolera w systemie nie miała wpływu na normalne działanie pozostałych kontrolerów
7. **System kontroli dostępu powinien posiadać świadectwo dopuszczenia CNBOP w celu odpowiedniego połączenia z SSP. Zwalnianie przejeżdżających KD odbywa się poprzez podanie sygnału sterującego z SSP bezpośrednio na kontroler.**
8. System kontroli dostępu oferuje konfigurowalne harmonogramy czasowe umożliwiające elastyczne programowanie automatycznego blokowania i odblokowania dowolnych drzwi, a także włączanie i wyłączanie ustawień posiadacza karty w celu ograniczenia możliwości wejścia do określonych obszarów dla dowolnej grupy dostępu w zaprogramowanych godzinach
9. Harmonogram czasowy zawiera funkcję dni świątecznych umożliwiającą użytkownikowi programowanie świąt narodowych oraz definiowanie własnych świąt. Wszystkie harmonogramy są definiowane w oparciu o dzień, godziny i minuty

#### URZĄDZENIA

1. System kontroli dostępu powinien być rozbudowywalny do przynajmniej 1200 czytników.
2. Komunikacja sterowników kontroli dostępu z serwerem zarządzającym powinna odbywać się za pomocą TCP/IP
3. Sterowniki systemu kontroli dostępu w przypadku utraty połączenia z serwerem (praca offline/autonomiczna) zarządzającym powinny realizować swoje funkcje normalne
4. Podczas pracy offline, każdy sterownik kontroli dostępu powinien być w stanie przechować przynajmniej 1 000 000 zdarzeń (jeden milion), które w momencie powrotu komunikacji z serwerem, będą wysłane do bazy danych oprogramowania zarządzającego.
5. Sterowniki kontroli dostępu powinny monitorować status zasilania baterijnego, zasilania sieciowego AC oraz napięcia DC między zasilaczem a samym sobą. Wspomniane informacje powinny być raportowane do oprogramowania zarządzającego
6. Sterowniki kontroli dostępu powinny mieć możliwość pracy w sieci LAN oraz WAN
7. Każdy sterownik powinien być wyposażony w wejścia służące do obsługi np. kontaktronów, przycisków wyjścia uprawnionego oraz w wyjścia przekaźnikowego do np. sterowania drzwiami.
8. Każde wyjście przekaźnikowe w sterowniku powinno mieć możliwość niezależnej konfiguracji pracy potencjałowej bądź bez potencjałowej
9. Każde wejście powinno posiadać możliwość parametryzacji przy pomocy do dwóch rezystorów
10. Sterownik kontroli dostępu obsługuje połączenia z interfejsem RS485

#### Oprogramowanie systemu KD (moduł SMS)

1. Oprogramowanie zarządzające systemem kontroli dostępu powinno pracować w architekturze klient-serwer
2. Aplikacja serwerowa powinna wspierać architekturę 32bit oraz 64bit
3. Oprogramowanie systemu kontroli dostępu powinno wspierać standardy IT takie jak OPC, AutoCAD, LDAP, HTML, ASP.NET
4. Oprogramowanie powinno rejestrować zdarzenia w bazie danych MSSQL
5. Oprogramowanie powinno mieć możliwość wyboru, jakie typy zdarzeń mają być rejestrowane w bazie MSSQL

6. Oprogramowaniem zarządzające powinno mieć możliwość współpracy z bazą danych MSSQL zainstalowaną na tym samym komputerze jak również na komputerze zdalnym (taka konfiguracja może być podyktowana wydajnością serwerów)
7. Wizualizacja
  - 7.1. Wizualizacja elementów systemu kontroli dostępu powinna być realizowane w oparciu o mapy wektorowe np. AutoCad
  - 7.2. Z poziomu mapy wizualizacyjnej operator powinien mieć łatwy dostęp do komend sterujących jak:
    - 7.2.1. Otwórz drzwi jednorazowo
    - 7.2.2. Otwórz drzwi na stałe
    - 7.2.3. Zablokuj drzwi
    - 7.2.4. Zablokuj czytnik
    - 7.2.5. Wysteryluj przekaźnik
    - 7.2.6. Pokaż ostatnie zdarzenia jakie miały miejsce na urządzeniu
  - 7.3. Ikony przedstawiające poszczególne elementy systemu (drzwi, czytniki, sterowniki,...) powinny być możliwe do zmiany
8. Interfejs graficzny operatora
  - 8.1. Powinien być edytowalny w celu dostosowania go do potrzeb i uprawnień operatora
  - 8.2. Powinna być możliwość dodania przycisków wykonujących wybrane komendy na wybranej grupie urządzeń
9. System powinien mieć możliwość alarmowania przynajmniej o:
  - 9.1. Wyważeniu drzwi
  - 9.2. Zbyt długim otwarciu drzwi
  - 9.3. Utracie komunikacji z dowolnym sterownikiem
  - 9.4. Użycie karty z czarnej listy
  - 9.5. Użycie karty bez uprawnień
  - 9.6. Użycie karty nieznanej
  - 9.7. Użyciu karty o określonym numerze**
  - 9.8. Błędny kod PIN
  - 9.9. Karta poza trasą
  - 9.10. Alarm sabotażowy sterownika
  - 9.11. Antipassback
  - 9.12. Ważność uprawnień wygasła
  - 9.13. Wyrwykowa kontrola
10. Oprogramowanie w momencie wykrycia istotnego zaprogramowanego zdarzenia alarmowego powinno mieć możliwość:
  - 10.1. Powiadomienia operatora sygnałem dźwiękowym
  - 10.2. Automatycznego wykonania zbliżenia na mapie na urządzenie, które jest w stanie alarmu
  - 10.3. Wyświetlenia dokumentu alarmowego np. z procedurą postępowania na wypadek danej sytuacji
  - 10.4. Wyświetlenie dodatkowej warstwy graficznej na mapie na wizualizacyjnej np. dróg ewakuacyjnych na wypadek pożaru
  - 10.5. Wykonać komendy sterujące (np. Zablokować drzwi, wysterylować przekaźnik)
11. Oprogramowanie powinna zapewniać możliwość definiowania obszarów logicznych w obiekcie (np. serwerownia, biuro itd.) w celu monitorowania położenia posiadaczy kart
12. Kolejność przejść - system powinien udostępniać funkcję sprawdzania kolejności dostępu, która umożliwia uprawnionemu posiadaczowi karty wejście przez drzwi lub grupę drzwi należącą do zdefiniowanego obszaru tylko, kiedy osoba przeszła już przez inne określone drzwi
13. Śluza – system powinien posiadać funkcję śluzy umożliwiającą zarządzanie dwoma lub więcej powiązаныmi drzwiami sterowanymi przez dwie pary lub więcej czytników (we / wy) lub czytniki wejścia oraz przycisk żądania wyjścia. W tym samym momencie mogą być otwarte tylko jedne drzwi. Tak długo jak jedne drzwi są otwarte, pozostałe będą zablokowane przed dostępem

#### 14. Uprawnienia operatora

14.1. Oprogramowanie powinno umożliwiać skonfigurowanie indywidualnych uprawnień operatora

##### 14.1.1. Uprawnienia odnośnie danych użytkowników

- 14.1.1.1. Widoczność
- 14.1.1.2. Odczyt
- 14.1.1.3. Modyfikacja
- 14.1.1.4. Usuwanie
- 14.1.1.5. Dodawanie

Wyjaśnienie: powinna być możliwość tak skonfigurowania uprawnień operatora, aby mógł tylko odczytać określone dane użytkownika i je zmodyfikować ale aby nie mógł usunąć karty.

##### 14.1.2. Uprawnienia odnośnie komunikowanych zdarzeń do operatora:

- 14.1.2.1. Pokaż własne komunikaty
- 14.1.2.2. Pokaż komunikaty bez danych osobowych
- 14.1.2.3. Pokaż wszystkie komunikaty

##### 14.1.3. Uprawnienia odnośnie widocznych na mapie wizualizacyjnej elementów

##### 14.1.4. Uprawnienia odnośnie widocznych map wizualizacyjnych

#### Kontroler KD

Parametry podstawowe:

Sprzęt	Procesor RENESAS M32C84 Pamięć EPROM / FLASH 512 kB Pamięć SRAM 256 kB Pamięć szeregową EEPROM Zegar RTC Dołączana karta Compact Flash 2 GB Bateria do zasilania pamięci SRAM i zegara RTC Adres hosta można ustawić za pomocą przełącznika suwakowego Interfejs hosta: <ul style="list-style-type: none"><li>- RS485 (2- lub 4-żyłowy) z transoptorami</li><li>- RS232</li><li>- Ethernet 10/100BaseT (TCP/IP) ze złączem RJ45</li></ul> 4 interfejsy czytników: <ul style="list-style-type: none"><li>- RS-485, 2-żyłowy, transoptory, 19 200 bodów</li></ul> 8 wyjść przełącznikowych: <ul style="list-style-type: none"><li>- maks. napięcie przełączania: 30 VDC</li><li>- maks. prąd przełączania: 1,25 A</li></ul> 8 monitorowanych wejść analogowych Zabezpieczenie antysabotażowe Przycisk resetowania
Temperatura	0°C ÷ +45°C
Zasilacz	10 ÷ 30 VDC, maks. 60 VA
Klasa ochrony	IP 30

Podstawowe funkcje:

#### Przechowywanie poniższych danych

- Dane główne
- Autoryzacje
- Uprawnienia dostępu
- Wyświetlany tekst
- Konfiguracje czytników

#### Interpretacja danych transakcji z czytnika

- Kontrola autoryzacji
- Żądania komputera
- Kod PIN

#### **Kontrola / monitoring:**

- Brak zezwolenia lub zezwolenie na wejście
- Wyzwalanie alarmu
- Stany drzwi
- Stany pracy czytników
- Stany alarmu wewnętrznego

#### **Wysyłanie komunikatów**

- Żądania komputera
- Dane transakcji do zachowania
- Komunikaty o błędach i usterkach
- Komunikaty alarmowe

#### **Dostarczanie zasilania dla następujących elementów:**

- Czytniki
- elektrozaczepy
- Zaciski do zasilania styków

### **Czytnik kart**

Parametry podstawowe:

<b>Charakterystyka elektryczna</b>	
Napięcie wejściowe	8,5 V do 16 VDC – maks. 18 VDC
Pobór mocy	65 mA przy 12 VDC Maks.: 130 mA przy 12 VDC
<b>Charakterystyka działania</b>	
Wyjście układu antysabotażowego	Otwarty kolektor, aktywny poziom niski, maks. prąd upływu 32 mA. Technologia optyczna
Wyjście Wiegand D0	5 V (TTL)
Wyjście Wiegand D1	5 V (TTL)
Wejście sterowania zielonej diody LED	Aktywny poziom niski
Wejście sterowania czerwonej diody LED	Aktywny poziom niski
Wejście sterowania sygnału dźwiękowego	Aktywny poziom niski
RS485	Protokół OSDP
<b>Parametry środowiskowe</b>	
Środowisko pracy	W pomieszczeniach i na zewnątrz — każde warunki atmosferyczne.
Temperatura pracy	-25°C do 65°C (-13°F do 150°F)
Wilgotność podczas pracy	0 do 95% (bez kondensacji)
Stopień ochrony	IP65
Odporność na promieniowanie UV	Tak
<b>Dane techniczne MIFARE i kart</b>	
Zasięg odczytu — karty ISO	> 6 cm
Pilot	> 2 cm
Obsługiwane karty	MIFARE 13,56 MHz ISO 14443, typ A
Zabezpieczenie antykolizyjne	Tak
Obsługa układów scalonych NXP	MF1ICS20 — 320 bajtów MF1ICS50 — 1K MF1ICS70 — 4K
<b>Obsługa MIFARE MAD i CSN</b>	
Czytnik zgodny z regułami MAD	
Odczytuje INIT CSN	Tak
Odczytuje CSN w przypadku niewykrycia danych MAD	Tak

## MONTAŻ URZĄDZEŃ

Dokładne rozmieszczenie urządzeń zostało pokazane na planie instalacji KD.

Wszystkie elementy instalacji powinny być oznaczone alfanumerycznie, w sposób trwały. Nie dopuszcza się oznaczeń w postaci pisania na powłokach kablowych, należy stosować specjalne trwałe oznaczniki. Te same oznaczenia powinny być użyte w urządzeniach monitorujących, sterujących, wizualizujących system oraz w dokumentacji powykonawczej.

Przewody należy instalować tak, aby chronić je przed uszkodzeniami w rurkach ochronnych możliwie z dala od instalacji mogących mieć wpływ na funkcjonowanie systemu. Przejścia przewodów instalacji przez ściany zewnętrzne oraz wewnętrzne pomiędzy strefami pożarowymi uszczelniać przy pomocy mas uszczelniających o odporności właściwej dla ścian, które są uszczelniane.

Montaż wszystkich urządzeń wykonać zgodnie z DTR poszczególnych urządzeń oraz według wytycznych producenta.

## ZALECENIA URUCHAMIANIA, EKSPLOATACJI I KONSERWACJI

Przed przekazaniem systemu do eksploatacji zaleca się dokładne sprawdzenie systemu i przeprowadzenie prób funkcjonalnych oraz przeprowadzenie pomiarów sprawdzających wszystkich łączy. Należy również wykonać dokumentację powykonawczą oraz przeszkolić pracowników obsługujących system.

### Zestawienie podstawowych materiałów:

Lp.	Opis	Ilość
1.	Kontroler RS485 z Kartą CF	4
2.	płyta rozszerzeń 8-wejść 8-wyjść	4
3.	Zasilacz z dodatkową przetwornicą do czytników, na 2 moduły KD	4
4.	Akumulator 12V/18Ah, certyfikat VdS	8
5.	Czytnik, MiFare classic	31
6.	Czytnik administracyjny	1
7.	Karty MIFARE Classic 1kB ISO (50 sztuk)	1
8.	Miniaturowy kontakt magnetyczny do montażu powierzchniowego (biały), przyklejany, wymiary (dł x szer x głęb) 4,8 x 6,35 x 27 mm, szczelina 15.24 mm, z bocznym przewodem, paczka po 10szt.	37
9.	Przycisk ewakuacyjny z osłoną	9
10.	Przycisk wyjścia natynkowy	2
11.	Elektrozaczep symetryczny rewersyjny	24
12.	Licencja podstawowa	1
13.	Licencja 32 drzwi (do licencji podstawowej )	1

## 18. INSTALACJA TELEWIZJI DOZOROWEJ

Instalacja telewizji dozorowej zakłada obserwację elewacji, stref komunikacyjnych oraz wybranych pomieszczeń. Wewnątrz budynku przewidziano wykorzystanie kamer IP, wewnętrznych, kopułkowych, z zasilaniem PoE. Na zewnątrz budynku, zamontowane zostaną kamery zewnętrzne IP, z zasilaniem PoE. Kamery zewnętrzne należy zamontować na elewacjach budynku, na wysokości ok. 3,5 m nad terenem.

Z szafy CCTV do każdej kamery należy doprowadzić oddzielny przewód typu FTP, kategorii 6. Przewody należy prowadzić w rurkach i korytkach przewidzianych dla instalacji słaboprądowych.

### Wymagania ogólne dla systemu monitoringu wizyjnego

Projektowany system telewizji dozorowej musi być zbudowany w oparciu o infrastrukturę sieciową wykorzystując do tego kamery IP, serwery sieciowe, macierze iSCSI. Wszelkie serwery powinny być wyposażone w system operacyjny co najmniej Windows Server 2019. Niedopuszczalne jest stosowanie rozwiązań starszych z uwagi na zakończone lub kończące się w niedługim czasie wsparcie producenta systemu operacyjnego. Serwery i macierze powinny pochodzić z oferty jednego producenta lub być przez producenta kamer, oprogramowania dostosowane i zoptymalizowane do poprawnej pracy.

System telewizji dozorowej powinien pochodzić z oficjalnego kanału sprzedaży, z jawnej dystrybucji.

Wraz ze wszystkimi komponentami systemu powinna być dostarczona dokumentacja w języku polskim. Wymaga się aby w języku polskim dostępne były co najmniej dokumenty: Deklaracja zgodności, karta katalogowa, instrukcja obsługi, instrukcja instalacji. Wszelka dokumentacja powinna być dostępna na co najmniej na stronie producenta bez konieczności rejestracji czy logowania.

Producent powinien posiadać zaplecze techniczne oraz dział techniczny. Producent powinien gwarantować dostęp do szkoleń technicznych w dotyczących kamer, szkoleń uruchomieniowych oraz obsługi. Szkolenia muszą odbywać się w formie warsztatów w siedzibie producenta lub dystrybutora. Szkolenia muszą kończyć się oficjalnym dokumentem potwierdzającym zdobyte umiejętności. Dokument powinien być wystawiony po potwierdzeniu zdobytej wiedzy, np. poprzez egzamin końcowy. Wymaga się aby system był instalowany i uruchamiany przez osoby posiadające odpowiednie kwalifikacje potwierdzone udziałem i certyfikatem szkoleniowym wystawionym przez producenta.

Urządzenia i oprogramowanie zarządzające powinny być zgodne ze standardami ONVIF. Zgodność tą należy potwierdzić obecnością na liście produktów kompatybilnych dostępnej na oficjalnej stronie standardu [onvif.org](http://onvif.org). Wymaga się aby urządzenia pochodziły od producenta sklasyfikowanego jako Full Member co ma zagwarantować iż producent dokłada wszelkich starań aby produkowane rozwiązania były kompatybilne z najnowszymi standardami ONVIF oraz iż producent wyznacza nowe standardy i kierunki rozwoju onvif.

Producent powinien oferować 5 letnią gwarancję na urządzenia. Producent musi posiadać własne zaplecze serwisowe na terenie EU.

Producent w ramach dostarczonego systemu powinien zapewniać możliwość skonfigurowania systemu tak aby zapewniał pełne szyfrowanie end-to-end, czyli od kamery przez serwer, macierze i stacje robocze.

W ramach pracy w systemie kamery powinny wspierać i obsługiwać infrastrukturę klucza publicznego PKI. Ma to zagwarantować odpowiedni poziom bezpieczeństwa pracy urządzenia w systemie.

Kamera sieciowa musi mieć wbudowany moduł Secure Element z funkcją Trusted Platform Module (TPM). Sprzęt bezpiecznie przechowuje wszystkie certyfikaty i klucze kryptograficzne potrzebne do uwierzytelniania i szyfrowania. W zależności od modelu kamery, Secure Element obsługuje klucze szyfrowania RSA o długości do 4096 bitów, zapewniając bezpieczeństwo danych po 2030 roku z wykorzystaniem szyfrowania AES 256bit. Projektowana kamera musi umożliwiać współpracę z serwerem RADIUS z wykorzystaniem protokołu autoryzacji 802.1x.

W celach ułatwienia zarządzania dostępem do kamer wymaga się aby wspierały one funkcję ActiveDirectory. Dzięki temu w rozległych sieciach i zaawansowanych instalacjach zarządca systemu dostaje proste, globalne narzędzie zarządzania użytkownikami.

W celu zagwarantowania najlepszej jakości obrazu wymaga się aby kamera spełniała szereg kryteriów oraz parametrów opisanych w wymaganiach. Kluczowe parametry kamer powinny być mierzone i podawane zgodnie z powszechnie dostępną i uznawaną normą EN 62676-5.

Z racji dużej liczby kamer w systemie monitoringu, celem zachowania efektywności systemu bez znaczącego zwiększenia liczby operatorów przyjmuje się aktywne wykorzystanie mechanizmów zaawansowanej analizy obrazów dla kamer CCTV, także dla kamer obrotowych. Tym samym wszystkie kamery w systemie będą wyposażone w funkcje inteligentnej analizy obrazu. Analiza obrazu odbywa się bezpośrednio w kamerze, dzięki czemu zapewniona jest najwyższa skuteczność (praca na nieskompresowanym obrazie) oraz skalowalność. W ramach konfiguracji kamery powinny być zaszyte przykładowe scenariusze analiz wideo. Ma to na celu przyspieszenie procesu konfiguracji reguł analitycznych w kamerach. Kamery powinny mieć możliwość ustawienie nawet 16 analiz wideo, różnych reguł alarmowania dla różnych klas obiektów. Dzięki inteligentnej technologii dostępnej w urządzeniach końcowych użytkownicy mogą ograniczać szerokość pasma i ilość pamięci masowej w przypadku braku akcji oraz przełączać się z powrotem na pełną jakość obrazu w przypadku alarmów wynikających z analizy obrazu. Stan alarmowy może być sygnalizowany za pomocą wyjścia przekątnikowego w urządzeniu lub połączenia alarmowego i transmitowany w postaci strumienia wizyjnego do dekodera lub systemu zarządzania sygnałem wizyjnym. Alarmy mogą być również kierowane do systemu zarządzania sygnałem wizyjnym w celu inicjowania rozbudowanych scenariuszy alarmowych.

#### **Zarządzanie i funkcje zdalne:**

W celu konfiguracji kamer producent powinien dostarczać odpowiednie narzędzie w postaci oprogramowania konfiguracyjnego. Oprogramowanie powinno być instalowane co najmniej na komputerach z systemem Windows. Oprogramowanie to powinno dawać możliwość wyszukiwania wielu kamer i innych urządzeń producenta, zmiany adresów IP, zmiany wszystkich ustawień kamery. Dodatkowo oprogramowanie musi zapewniać możliwość łatwej konfiguracji reguł analitycznych dostępnych w kamerach.

Oprogramowanie powinno zapewnić możliwość aktualizacji oprogramowanie układowego (firmware) kamer. Aktualizacja powinna odbywać się dla wszystkich kamer w systemie.

Kamery oraz wybrane urządzenia rejestrujące powinny dawać możliwość podłączenia do zewnętrznej usługi dostarczanej przez producenta - służącej do bieżącego monitorowania stanu urządzeń. Połączenie to powinno być bezpieczne, nie powinno wymagać podawania haseł ustawionych w kamerze. Preferowanym rozwiązaniem jest autoryzacja usługi w kamerze, serwerze. Serwery na których świadczona jest usługa zdalnego dostępu muszą być umieszczone i uruchomione w krajach UE.

Bezpieczne połączenie musi być realizowane poprzez zaszyte mechanizmy negocjacji uwierzytelnienia usługi do urządzeń. Dodatkowo usługa z reguły nie powinna wymagać odblokowywania portów. Odblokowywanie portów uznaje się za wprowadzenie luki w bezpieczeństwie systemu.

Usługa zdalnego monitorowania powinna dawać też możliwość zapisania pobrania i przechowywania w chmurze konfiguracji dla kamer. Dzięki temu wszelkie pliki z konfiguracją są przechowywane w bezpiecznym miejscu, a dostęp do nich nie zależy od miejsca połączenia do usługi.

Usługa powinna umożliwiać przeprowadzenie zdalnego audytu wszelkich podłączonych urządzeń. W ramach audytu niezbędne jest wskazanie status połączenia, nagrywanie, alerty o nowych firmware kamer. Alerty te powinny być wyświetlane w postaci czytelnych ikon.

Usługa powinna umożliwiać odczytanie stanów komponentów urządzenia rejestrującego: pracy wentylatorów, dysków, kontrolera RAID, obudowy.

Usługa musi mieć możliwość skonfigurowania reguł powiadomień na różnego rodzaju zdarzenia w systemie. Poprzez zdarzenia rozumie się: utratę połączenia z kamerą, problemy z nagrywaniem, dostępne nowe aktualizacje oprogramowania zarządzającego, dostępne nowe oprogramowania układowe kamer (firmware), stany techniczne rejestratora jak otwarcie obudowy, stan RAID.

#### **Normy i wytyczne:**

Zakład się iż projektowany system monitoringu wizyjnego musi spełniać szereg norm oraz wytycznych rynkowych. Dla całości system wymaga się aby został zaprojektowany zgodnie z wymaganiami stawianymi przed typem obiektu określonym w normie EN 67676-1.

Od systemu zarządzania VMS wymaga się aby spełniał wymagania określone w normie EN 62676-4 dla systemów z GRADE 4.

Zarówno oprogramowanie jak i kamery powinny być kompatybilne z ONVIF i potwierdzone na oficjalnej stronie organizacji [www.onvif.org](http://www.onvif.org).

W przypadku kompresji oczekuje się wsparcia dla H.264 zgodne z ISO/IEC 14496-10 oraz H.265 zgodne z HEVC.

#### **Możliwości integracji:**

Projektowane kamery muszą wspierać protokół MQTT. Jest to protokół dedykowany do lekkiej integracji urządzeń automatyki przemysłowej. Implementacja tego protokołu w kamerach daje proste narzędzie doysterowania elementów automatyki przemysłowej bez konieczności implementacji pełnego API/SDK. Poprzez protokół MQTT kamera powinna wysyłać informacje o zdarzeniach analitycznych, wyzwolonych regułach, typie obiektu, stanie nagrywania czy stanie wyjścia/wejścia przekaźnikowego. Na tej podstawie serwer integrujący (serwer MQTT) jest w stanieysterować inne dowolne podpięte urządzenie.

Integracja z systemem napłotowym: Poprzez wykorzystanie MQTT w kamerach istnieje możliwość prostej integracji z systemem napłotowym. Wymaga się aby sterownik napłotowy również wykorzystywał MQTT. Dzięki takiemu zastosowaniu użytkownik zyskuje narzędzie do prostej konfiguracji/integracji obu systemów. Kamera poprzez protokół MQTT wysyła informacje o typie obiektu a odbiornik tej informacji jest w stanieysterować odpowiednio lampę lub szereg lamp. W przypadku detekcji pojazdówysterowane zostaną tylko niektóre lampy.

Integracja z oświetleniem: Poprzez wykorzystanie MQTT w kamerach istnieje możliwośćysterowania oświetlenia na obiekcie w zależności od typu wykrytego obiektu. Kamera poprzez protokół MQTT wysyła informacje o typie obiektu a odbiornik tej informacji jest w stanieysterować

odpowiednio lampę lub szereg lamp. W przypadku detekcji pojazdówysterowane zostaną tylko niektóre lampy.

Kamery powinny mieć możliwość komunikacji między sobą poprzez wykorzystanie języka skryptów lub innego mechanizmu równoważnego. Istotne jest iż do komunikacji pomiędzy kamera nie jest wymagane żadne dodatkowe oprogramowanie, poza oprogramowaniem do samej konfiguracji. Kamery po wystąpieniu dowolnego zdarzenia powinny mieć możliwość co najmniej -ysterowania wyjść przekaźnikowych w innej/innych kamerach,ysterowanie kamery PTZ w ustaloną pre-pozycję itp.

Producent kamer musi dostarczyć na żądanie dokumentację API/SDK umożliwiającą integrację kamery w obcym środowisku. Udostępnienie dokumentacji może wymagać podpisania dokumentu NDA, lecz nie może być płatne. Wraz z dokumentacją producent gwarantuje wsparcie przy integracji w postaci konsultacji co najmniej mailowych z działem technicznym producenta lub działem integracji.

Kamery muszą mieć możliwość integracji z głośnikami IP. Integracja musi umożliwiać odtworzenie do 16 różnych komunikatów automatycznie przypisanych do 16 różnych stref detekcji, analiz wideo itp. Działanie głośnika z kamerą powinno odbywać się w sposób autonomiczny tj. poprzez zaprogramowane scenariusze działań. Scenariusze działań powinny być budowane w oparciu o skrypty wbudowane w kamerę.

Zakłada się iż w zależności od strefy alarmu odtwarzany będzie różny komunikat dźwiękowy.

#### **Rejestrator 64 ch**

#### **Wymagania projektowe**

##### **Serwer rejestracji**

1. Do rejestracji obrazu z kamer w systemie planuje się wykorzystanie dedykowanej macierzy dyskowej, służącej jako przestrzeń dyskowa do zapisu.
2. Urządzenie jest przeznaczone do bezpośredniego montażu w szafie rack.
3. Serwer rejestrujący jest dostarczony od producenta w formie prekonfigurowanej, w formie gotowej do podłączenia do oprogramowania zarządzającego.
4. Pojedynczy serwer umożliwia podłączenie, zarządzanie i rejestrację do 64 kamer (kanałów wideo) w systemie.
5. Serwer jest wyposażony w dyski SATA-3 do rejestracji, do których zapewniony jest dostęp od frontu urządzenia, umożliwiając łatwą wymianę dysków.
6. Serwer posiada wbudowany transkodery, umożliwiające wykorzystanie technologii transkodowania dynamicznego, dopasowującego parametry strumienia wizyjnego, przekazywanego do aplikacji klienckich, do aktualnych możliwości łącza.
7. Serwer rejestrujący wspiera technologie SNMP, zdalnego pulpitu czy monitorowania http elementów sprzętowych i aplikacji zarządzającej.
8. Serwer powinien być objęty co najmniej 5-letnią gwarancją producenta.
9. Podstawowe parametry techniczne serwera zestawiono w poniższej tabeli:

Parametr	Wymagania minimalne
Funkcja	Serwer do zarządzania systemem i rejestracji nagrań
Oprogramowanie	System zarządzania wideo, zgodny z wymaganiami poniżej, pracujący na serwerze
Stacje klienckie	Do 10 aplikacji klienckich podłączonych jednocześnie
System operacyjny	Microsoft Windows Server IoT 2022
Dysk systemowy	256 GB M.2 SSD
Wbudowana przestrzeń dyskowa	4x8TB
Maksymalna pojemność wbudowanej	64TB

przestrzeni dyskowej	
Możliwość rozbudowy o zewnętrzne macierze dyskowe	Do 4 dodatkowych macierzy dyskowych w systemie w obrębie danego serwera zarządzającego.
Zabezpieczenie przed usterką dysków twardych	RAID 5, RAID 5 + Hot Spare lub RAID 6
Procesor	Intel® Core™ i3-10100E
Pamięć RAM	16GB DDR4-2933 2Rx8 ECC UDIMM
Maksymalna przepustowość	Do 400 Mb/s
Interfejs sieciowy	2 x Gigabit Ethernet
Nagrywarka DVD	Wbudowana
Sposób montażu	1U
Zasilanie	230VAC, 350W

### Wymagania projektowe

#### System zarządzania wideo (VMS)

#### System rejestracji

- System zarządzający umożliwia obsługę kamer i enkoderów, realizujących funkcję rejestracji bezpośrednio przez urządzenie końcowe, w celu bezpośredniej rejestracji strumienia wideo z kamery na przestrzeni dyskowej iSCSI.
  - System zarządzający nie jest odpowiedzialny w takim przypadku za przetwarzanie strumienia czy rejestrowanych danych
- System zarządzania umożliwia jednoczesne zarządzanie wieloma urządzeniami rejestrującymi.
- Przestrzeń dyskowa oraz opcje zapisu w razie usterki mogą być konfigurowane z poziomu konfiguratora oprogramowania zarządzającego.
- System zarządzający umożliwia rejestrację kamer zgodnych z ONVIF Profile S za pośrednictwem rejestratora serwerowego, zapisującego nagrania na przestrzeni dyskowej iSCSI.
- System umożliwia zarządzanie wszystkimi dostępnymi macierzami dyskowymi w konfiguracji pojedynczej puli lub wielu dostępnych puli zapisu.
- Przestrzeń dyskowa, w obrębie dostępnej puli zapisu, będzie przypisywana w sposób dynamiczny podłączonym kamerom, enkoderom, czy rejestratorom. Nie zachodzi przy tym potrzeba stałego przypisania kamer czy enkoderów do wybranej i określonej macierzy dyskowej. Dzięki temu zagwarantowane jest optymalne wykorzystanie dostępnej przestrzeni, jak również równomierne obciążenie sieci i urządzeń.
- Transfer danych z enkoderów, kamer i rejestratorów jest kontrolowana w oparciu o dostępną przepustowość łącza sieciowego oraz wydajność danej macierzy dyskowej.
- W razie trwałej usterki kamery, zapisane nagrania mogą być przypisane ponownie do podłączonego, nowego urządzenia.
- W przypadku nagrywania alarmowego, buforowanie fragmentu nagrań przed wystąpieniem alarmu może odbywać się w kamerze IP, wyposażonej w pamięć podręczną, a fragment ten zostanie zapisany na macierzy dyskowej jedynie po wystąpieniu alarmu, aby ograniczyć obciążenie sieci.
- Możliwe jest skonfigurowanie do 7 rodzajów rejestracji przed wystąpieniem alarmu dla każdej kamery IP, w zależności od różnych zdarzeń lub zdarzeń złożonych.
- System rejestracji obsługuje urządzenia, umożliwiające bezpośrednią rejestrację, z wykorzystaniem protokołu iSCSI.
- Kamery, wykorzystujące funkcję samodzielnej rejestracji na przestrzeni dyskowej, są w stanie samodzielnie rejestrować nagrania na macierzy, bez pośrednictwa serwera czy dodatkowego rejestratora.

13. Kamery wykorzystują mechanizm lokalnego buforowania, umożliwiający redukcję wpływu krótkotrwałych przerw w transmisji sieciowej i rejestrację bez utraty fragmentów nagrań.
14. System zarządzania wideo umożliwia pełną obsługę kodowania h.264 oraz h.265.
15. System zarządzania wideo umożliwia konfigurację alarmu, gdy dojdzie do ręcznego usunięcia zarejestrowanych nagrań wideo.

### **Skalowalność**

1. Komponenty programowe systemu zarządzania wideo mogą być uruchomione zarówno na pojedynczym komputerze, jak i na osobnych maszynach i serwerach, dla spełnienia wymagań w przypadku dużych systemów.
2. Pojedynczy serwer VMS umożliwia obsługę do 64 kamer/enkoderów.

### **Niezawodność i odporność na awarie**

1. System zarządzania wideo powinien wspierać funkcję automatycznego buforowania lokalnie w razie usterki połączenia sieciowego
  - a. Nagrania są buforowane w pamięci (karcie SD) kamery IP w razie braku komunikacji sieciowej. System zarządzania umożliwia alarmowanie, gdy kończy się dostępna przestrzeń rejestracji lub nagrania są usuwane z racji niewystarczającej przestrzeni dyskowej. Po przywróceniu komunikacji sieciowej, kamera automatycznie uzupełnia nagrania na macierzy dyskowej. Proces ten powinien odbywać się automatycznie i nie wymaga udziału użytkownika
2. System zarządzania wideo powinien gwarantować, że nagrania nie zostaną w żaden sposób naruszone w przypadku usterki serwera.
3. System zarządzania powinien umożliwiać dalszą pracę, w tym podgląd na żywo, odtwarzanie i eksportowanie nagrań, również w przypadku wyłączenia lub usterki serwera zarządzającego.
4. Aplikacja kliencka wskazuje status połączenia z serwerem zarządzającym.
  - a. Aplikacja kliencka powinna pracować dalej również, gdy serwer zarządzający jest niedostępny
  - b. Informowanie o statusie połączenia powinno obejmować stan połączony, rozłączony, czy brak synchronizacji konfiguracji aplikacji klienckiej względem serwera zarządzającego
  - c. Status połączenia z serwerem zarządzającym powinien być wskazany przy ikonie na liście urządzeń
5. System powinien być zaprojektowany w taki sposób, aby zmiany konfiguracji dowolnej części systemu nie zaburzały obsługi, zanim operator nie zdecyduje się na aktualizację i odświeżenie konfiguracji stacji roboczej.
6. System zarządzania wideo powinien cechować się wysokim stopniem odporności na awarie. Nawet w przypadku jednoczesnej usterki serwerów zarządzających oraz macierzy dyskowych, operatorzy powinni wciąż mieć możliwość podglądu obrazu z kamer i sterowania nimi, jak również odtwarzania nagrań z karty pamięci w kamerze lub innej formy rejestracji w razie awarii.
  - a. Niedostępność serwera zarządzającego nie może wpływać na stan rejestracji obrazu z kamer.

- b. Po ponownym uruchomieniu/podłączeniu brakujących komponentów systemu, nie jest wymagane żadne działanie użytkownika czy administratora w celu powrotu do normalnego trybu pracy systemu.
- 7. Operator powinien mieć możliwość uruchomienia aplikacji klienckiej nawet, gdy serwer zarządzający jest niedostępny.
- 8. System zarządzania wideo powinien gwarantować, że alarmy zostaną zapamiętane również po poprawnym, ponownym uruchomieniu serwera zarządzającego.

### **Oprogramowanie klienckie**

1. Stacje robocze systemu zarządzania wideo umożliwiają podłączenie do 4 monitorów, a każdy z monitorów może być niezależnie skonfigurowany do wyświetlania obrazu z kamer na żywo, odtwarzania nagrań, map lokalizacji lub zdarzeń alarmowych.
2. Aplikacja kliencka systemu zarządzania wideo udostępnia interfejs użytkownika do monitorowania i obsługi systemu. Aplikacja kliencka umożliwia podgląd na żywo, przeglądanie i pobieranie nagrań oraz obsługę alarmów.
3. Użytkownik ma możliwość przeszukiwania drzewa logicznego w poszukiwaniu nazw elementów systemu (na przykład kamery).
4. System zarządzania wideo oferuje każdemu z użytkowników niezależną listę zakładek
  - a. Lista zakładek umożliwia zapisanie zakresu czasowego lub określonego punktu w czasie dla późniejszej analizy i eksportu
  - b. Zakładki powinny być dostępne zarówno w trybie na żywo, jak i w trybie odtwarzania.
5. System zarządzania wideo oferuje każdemu z użytkowników niezależną listę ulubionych
  - a. Drzewo ulubionych powinno umożliwiać skonfigurowanie map, folderów i urządzeń oraz pełnych widoków (układ okien wideo z przypisanymi kamerami) przez każdego użytkownika w strukturze zdefiniowanej przez użytkownika
  - b. Drzewo ulubionych użytkownika powinno być dostępne niezależnie od komputera, na którym loguje się on do systemu
  - c. Możliwe jest dostosowanie różnych widoków dla każdego okienka obrazu za pomocą funkcji e-PTZ i zapisanie tak stworzonych widoków jako ulubiony
  - d. Podczas wybierania ulubionych na ekranie wyświetla się spersonalizowany podgląd na żywo tej samej kamery (kamer).
6. System zarządzania wideo powinien zawierać okno, które wyświetla zbiór okienek z podglądem. Układ musi zapewniać optymalizację zarówno dla monitorów standardowych (4:3), jak i panoramicznych (16:9).
  - a. W przypadku standardowych monitorów liczba okienek z podglądem na okno będzie się zmieniać w zakresie od 1 (pojedynczego wideo w pełnym oknie) do 25, ułożonych w siatkę 5x5. Dostępny musi być suwak pozwalający na zmianę rozmiaru siatki w zakresie 1x1, 2x2, 3x3, 4x4 i 5x5.
  - b. W przypadku monitorów szerokoekranowych liczba okienek z podglądem na okno może się zmieniać w zakresie od 1 do 30, ułożonych w siatkę 1x1, 3x2, 4x3, 5x4 i 6x5.
  - c. Liczba okienek z podglądem, dostępnych dla operatora, może być ograniczona w zależności od konfiguracji danej grupy użytkowników.
  - d. System zarządzania wideo powinien umożliwiać powiększanie lub zmniejszanie paneli obrazu w obrębie siatki. Przykładowo, w siatce 5x5 pojedynczy panel obrazu można powiększyć, aby wykorzystać cztery okienka podstawowej siatki, tworząc większe okno podglądu. Pozwala to operatorowi oglądać wideo w dowolnym wzorze utworzonym w strukturze siatki.
    - i. Operator nie jest ograniczony jedynie do wstępnie skonfigurowanych układów, ale powinien mieć również możliwość zmiany rozmiaru okna podglądu, klikając i przeciągając krawędź okienka obrazu, aby przeciągnąć granicę w poziomie lub w pionie lub klikając róg okienka obrazu, aby przeciągnąć róg okienka po przekątnej, do żądanego rozmiaru.
  - e. Aplikacja kliencka powinna umożliwiać wybranie i podświetlenie danego okienka podglądu.
    - i. Jedno z okienek podglądu aplikacji klienckiej powinno pozostawać wybrane i podświetlone

- ii. Wybrane i podświetlone okienko podglądu jest zawsze używane dla poleceń sterujących, np. natychmiastowego sterowania PTZ, sterowania odtwarzaniem nagrań oraz odtwarzania dźwięku
- 7. System zarządzania wideo powinien obsługiwać źródła dźwięku dla podłączonych kamer IP oraz enkoderów. Powinno być możliwe przypisanie źródeł audio do kamer.
  - a. Aplikacja kliencka powinna umożliwiać włączenie/wyłączenie odtwarzania dźwięku dla każdej kamery.
  - b. System zarządzania wideo powinien wspierać dwa różne tryby audio – jednoźródłowe oraz wieloźródłowe
    - i. W trybie jednoźródłowym odtwarzany jest jedynie dźwięk dla źródła, przypisanego do kamery w aktualnie wybranym okienku podglądu
    - ii. W trybie wieloźródłowym odtwarzany jest dźwięk dla wszystkich źródeł audio kamer, wyświetlanych w aplikacji klienckiej
- 8. Aplikacja kliencka systemu zarządzania wideo umożliwia korygowanie odkształceń i tworzenie widoków panoramicznych dla kamer 360°, zarówno przy podglądzie na żywo, jak i w trakcie odtwarzania nagrań.
  - a. Aplikacja kliencka powinna umożliwiaćysterowanie kamer 360° różnych producentów z wykorzystaniem protokołu ONVIF
- 9. Aplikacja kliencka systemu zarządzania wideo umożliwia wyświetlanie określonych, prekonfigurowanych scen (e-PTZ) dla kamer 360° lub 180°, w zależności od danego scenariusza alarmowego.
- 10. Aplikacja kliencka umożliwia opcjonalnie wyświetlenie informacji z funkcji inteligentnej analizy obrazu w kamerze, takich jak obszary detekcji ruchu, maski obiektu oraz trajektorie, zarówno przy podglądzie na żywo, jak i w trakcie odtwarzania nagrań.
- 11. System zarządzania wideo będzie w sposób graficzny wskazywał stany urządzeń przy ich ikonach na liście lub na mapie.
  - a. W przypadku kamer, wyświetlane będą informacje o następujących stanach: utrata sygnału wideo, utrata połączenia sieciowego, rejestrowanie nagrań, zakłócenia obrazu wideo, prześwietlenie obrazu, obraz zbyt ciemny, brak kalibracji obrazu oraz sygnał audio przypisany dla strumienia wideo
  - b. Dla przekaźników oraz wejść stykowych, wskazywany jest stan otwarcia lub zamknięcia.
- 12. Aplikacja kliencka umożliwia zagnieżdżenie i otwarcie w oknie aplikacji dla systemu Windows, dając operatorowi możliwość otwarcia wielu aplikacji w jednym oknie interfejsu systemu zarządzania wideo.
- 13. Aplikacja kliencka powinna umożliwiać sterowanie kamerami typu PTZ z wykorzystaniem:
  - a. Graficznego elementu sterującego („joystick’a”) do kontrolowania kąta obrotu, pochylenia, przybliżenia, przesłony, wyostżenia oraz poleceń pomocniczych
  - b. Kliknięcia i przeciągnięcia myszy wewnątrz okienka z podglądem obrazu
- 14. W przypadku wybranych kamer typu PTZ, oferujących funkcję automatycznego podążania za wykrytym obiektem, aplikacja kliencka powinna dawać możliwość uruchomienia tego typu funkcjonalności i śledzenia po kliknięciu na wybranym obiekcie w podglądzie na żywo.

#### **Odtwarzanie i przeglądanie nagrań**

- 15. System zarządzania wideo przy przeglądaniu nagrań wyświetla linię czasu i w sposób graficzny przedstawia przegląd nagrań, zapisanych na dysku
  - a. Linia czasu powinna odzwierciedlać za pomocą kolorów różne tryby nagrywania.
  - b. Możliwe jest elastyczne i płynne dostosowanie skali dla linii czasu przeglądanych nagrań.
  - c. Linia powinna w sposób kolorystyczny wskazywać zakres czasu, dla którego dostępne są nagrania.
  - d. Nagrania zabezpieczone przed nadpisaniem lub usunięciem powinny być oznaczone kreskowaniem
  - e. Przy linii powinno istnieć wskazanie informujące o dostępności strumienia audio, powiązanego z nagraniami w danym zakresie czasu
- 16. System zarządzania wideo obsługuje przeszukiwanie nagrań pod kątem ruchu w określonych przez użytkownika obszarach obrazu z kamery.
- 17. System zarządzania wideo wspiera przeszukiwanie nagrań co najmniej w oparciu o następujące kryteria: rozmiar obiektu, kolor obiektu, kierunek ruchu i prędkość oraz wykrycie obiektów wkraczających lub opuszczających wybrane obszary.

18. System zarządzania umożliwia przeszukiwanie nagrań na podstawie dowolnej kombinacji zakresu czasu/daty, rodzaju zdarzenia, priorytetu alarmu, stanu alarmowego oraz urządzenia (urządzeń).
  - a. Możliwe jest zapisanie i przywrócenie parametrów wyszukiwania
19. System zarządzania umożliwia wyszukiwanie danych tekstowych, przechwyconych z urządzeń typu bankomat, kasa, czytnik kodów kreskowych i innych. Możliwe jest przeszukiwanie bazy danych w oparciu o fragment tekstu i znaki zastępcze
  - a. Wyniki wyszukiwania są prezentowane w postaci listy a wybór danego wyniku powoduje bezpośrednie wyświetlenie nagrań zarejestrowanych w danym momencie wraz z danymi tekstowymi.
  - b. Dane tekstowe są wyświetlane w oknie podglądu danej, odtwarzanej kamery. Możliwe jest zatem jednocześnie wyświetlenie danych tekstowych dla wielu kamer.
  - c. Operator powinien mieć możliwość wyboru czy dane tekstowe powinny być wyświetlane po prawej stronie czy pod oknem podglądu.

### **Wydajność**

20. Aplikacja kliencka systemu zarządzania wideo powinna umożliwiać wyświetlanie kilku strumieni w bardzo wysokiej rozdzielczości bez ograniczenia płynności, dzięki wykorzystaniu dekodowania GPU dla wybranych kart graficznych Nvidia oraz Intel.
21. Aplikacja kliencka umożliwia dekodowanie ramek IP, IBP oraz IBBP w strukturze GOP strumienia.
22. Aplikacja kliencka umożliwia dekodowanie strumieni wideo z odległością 250 klatek pomiędzy kolejnymi ramkami bazowymi, umożliwiając skuteczne ograniczenie wielkości strumienia dla kamer, gdzie zachodzi taka potrzeba.
23. Wszystkie komponenty programowe systemu zarządzania wideo powinny być oparte o architekturę 64-bitową.
24. System zarządzania wideo daje użytkownikowi aplikacji klienckiej możliwość włączenia automatycznego przełączania pomiędzy strumieniami o wysokiej i niższej rozdzielczości w oknie podglądu, w celu zagwarantowania optymalnej wydajności sprzętowej przy pracy z systemem
  - a. Aplikacja kliencka automatycznie otworzy strumień o niższej rozdzielczości, gdy użytkownik aplikacji klienckiej otworzy kilka obrazów z kamer na jednym monitorze
  - b. Aplikacja automatycznie wyświetli strumień o wysokiej rozdzielczości, gdy operator otworzy obraz z danej kamery na pełnym ekranie lub gdy użyje funkcji przybliżenia (zoom cyfrowy) dla większej szczegółowości obrazu.

### **Obsługa map**

1. System zarządzający umożliwia tworzenie map lokalizacji z aktywnymi ikonami dla urządzeń (kamer, przekaźników sterujących, wejść przekaźnikowych i innych elementów systemu), uruchamiania poleceń dla skryptów, uruchamiania sekwencji kamer i z linkami do innych map lokalizacji.
  - a. Możliwe jest przybliżanie i oddalanie map dla wygodnej pracy z systemem
  - b. Wspierane formaty map to co najmniej DWF, PNG oraz PDF
2. Aktywne ikony umożliwiają takie skonfigurowanie, aby wyświetlona została nazwa urządzenia lub nazwa linku.
3. Status danego urządzenia jest przedstawiony w sposób graficzny przy odpowiedniej ikonie na mapie.
4. Możliwe jest skonfigurowanie priorytetów zdarzeń dla urządzeń tak, aby wizualizowane było tylko jedno zdarzenie dla danej ikony na mapie w momencie jednoczesnego wystąpienia wielu zdarzeń.
5. Po najechaniu kursorem myszy na ikonę na mapie aplikacja powinna wyświetlić podgląd widoku z danej kamery, dla łatwiej identyfikacji urządzenia
6. Menu kontekstowe, przypisane do ikony kamery typu PTZ na mapie, umożliwia wybranie określonych położeń zaprogramowanych.
7. Możliwe jest zaakceptowanie i usunięcie alarmu z danej kamery, korzystając z menu kontekstowego danej ikony na mapie.

### **Mapy interaktywne**

1. System zarządzający umożliwia wykorzystanie interaktywnych map online i usług geolokacyjnych, w oparciu o mapy Microsoft Here.

2. System umożliwia stworzenie własnych widoków, będących określonymi wycinkami z mapy, wraz z wizualizacją kamer znajdujących się w danym obszarze.
3. System umożliwia naniesienie na wykorzystywane interaktywne mapy online dodatkowych warstw z mapami własnymi – np. z rzutem wnętrza danego budynku.
  - a. System umożliwia naniesienie do 200 poziomów/warstw nadziemnych oraz do 20 poziomów/warstw poniżej poziomu gruntu.
  - b. System umożliwia naniesienie na każdy z poziomów dowolnych kamer, które będą na stałe przypisane do danego poziomu.
4. Operator ma do dyspozycji pole do szybkiego przeszukiwania mapy, np. w celu znalezienia określonej ulicy lub określonej kamery.
5. System daje możliwość zwizualizowania i wyświetlania na mapie zakresu sceny (kąta obserwacji) dla każdej z umieszczonych na mapie kamer.
6. W przypadku kamer obrotowych wizualizowany zakres obserwacji jest obracany automatycznie, wraz z obrotem kamery.

### **Asystent śledzenia osób i obiektów**

1. System daje możliwość uruchomienia dodatkowej funkcji asystenta śledzenia osób i obiektów.
2. Po uruchomieniu funkcji asystenta w aplikacji klienckiej dla danej kamery, system automatycznie wycinek mapy z najbliższym otoczeniem danej kamery, jak również okna wideo z czterech pobliskich kamer.
3. Obraz z okolicznych kamer w aplikacji klienckiej jest wyświetlany w sposób inteligentny i intuicyjny, w zależności od rzeczywistego rozmieszczenia okolicznych kamer względem aktywnej obecnie kamery głównej.
4. Wraz z przemieszczaniem się osoby lub obiektu, operator może poprzez dwukrotne kliknięcie przejść do kolejnej, okolicznej kamery. W efekcie, w sposób automatyczny dostosowany zostanie widok mapy, jak również dobrane zostaną kolejne kamery z najbliższego otoczenia.
5. W przypadku zastosowania kamer obrotowych, okoliczne kamery zostaną automatycznie skierowane w kierunku obserwacji kamery głównej.
6. Dodatkowo, operator ma możliwość łatwego skierowania okolicznych kamer obrotowych w określone miejsce, poprzez dwukrotne kliknięcie na mapie.
7. Asystent śledzenia osób i obiektów umożliwia na korzystanie z wielopoziomowych map online.

### **Dynamiczne maski prywatności (anonimizacja)**

1. System zarządzania wideo umożliwia tworzenie dynamicznych masek prywatności (anonimizacja) dla obiektów sklasyfikowanych jako osoby.
2. System umożliwia przypisanie poszczególnych uprawnień do kamer powiązanych z maskami prywatności (anonimizacją) do określonych grup użytkowników.
3. System rejestruje obraz bez masek prywatności a są one dynamicznie nakładane na stacjach operatorskich dla użytkowników i kamer z włączoną tą funkcją.
4. System daje możliwość używania dynamicznych masek prywatności (anonimizacji) w trybie na żywo, w odtwarzaniu oraz możliwość eksportu nagrań z maskami prywatności.
5. W zależności od konfiguracji sprzętowej system daje możliwość anonimizacji na stacji klienckiej do 16 kamer jednocześnie.

### **Zarządzanie alarmami**

6. System zarządzania wideo umożliwia tworzenie alarmów zależnych od harmonogramu.
7. System umożliwia przypisanie poszczególnych alarmów do określonych grup użytkowników.
8. System umożliwia replikację zdarzeń w taki sposób, że jedno zdarzenie fizyczne w systemie generuje liczne zdarzenia systemowe. Takie zdarzenie można niezależnie skonfigurować, by umożliwić niezależną obsługę alarmów różnych grupom operatorów lub w sposób zależny od harmonogramu czasowego.
9. System zarządzania powinien umożliwiać zaprogramowanie alarmów tak, aby w sposób selektywny, w zależności od stanu alarmowego lub grupy użytkowników, automatycznie wyświetlić obraz z kamery powiązanej ze zdarzeniem.
10. Okno alarmowe systemu umożliwia takie skonfigurowanie, by wyświetlony został podgląd na żywo, odtwarzanie nagrań, dokumenty tekstowe, mapy obiektów, pliki HTML lub witryny (adresy URL). Dla każdego alarmu możliwe jest skonfigurowanie jednego okna odtwarzania nagrań i jednej mapy.

11. System oferuje reakcję na alarm w czasie maksymalnie 2 sekund, gdy dostępna jest wystarczająca przepustowość sieci.
12. System umożliwia dystrybuowanie powiadomień o alarmach, poprzez wpisy na liście alarmowej interfejsu operatora, do wszystkich członków określonej grupy użytkowników.
  - a. Gdy alarm zostanie zaakceptowany przez danego użytkownika, zostanie usunięty z listy alarmowej innych użytkowników grupy
  - b. System umożliwia wycofanie potwierdzenia alarmu. W takim przypadku alarm pojawi się ponownie na liście alarmowej wszystkich członków grupy użytkowników, do której przypisany został alarm.
13. System umożliwia wysłanie wiadomości e-mail lub SMS w odpowiedzi na alarm.

#### **Dynamiczne zarządzanie uprawnieniami użytkowników**

1. System zarządzania wideo daje możliwość dynamicznego zarządzania uprawnieniami użytkowników na podstawie dowolnego odebranego sygnału alarmowego, zdarzenia w systemie, harmonogramu lub wywołania ręcznego.
2. System ma możliwość utworzenia do 4 poziomów zagrożenia w ramach których określone operatorzy będą mieli dynamicznie zmieniane uprawnienia.
3. Dynamiczna zmiana uprawnień użytkownika oraz powrót do uprawnień początkowych powinien móc odbywać się w sposób automatyczny np. w parciu o harmonogram czasowy.
4. Wśród scenariuszy zakłada się:
  - a. Zmiana uprawnień operatora w zależności od alarmów:
    - i. Detekcja obiektu w strefie ochrony perymetrycznej powinna dawać dostęp operatorowi do kamer standardowo niewidocznych dla operatora.
    - ii. Detekcja osób w pomieszczeniach wewnętrznych po godzinach pracy powinna dawać dostęp do kamer wewnętrznych. Zakłada się iż po godzinach pracy ochrona ma dostęp tylko do kamer zewnętrznych.
    - iii. Detekcja pojazdów przecinających odpowiednie strefy powinna dawać dostęp do funkcji systemu takie jak interaktywne mapy.
    - iv. Włączenie/wyłączenie funkcji dynamicznych masek prywatności/anonimizacji z przycisków funkcyjnych w interfejsie oprogramowania lub przez odpowiedni manipulator.

#### **Śledzenie zmian: Audit Trail**

1. System daje możliwość szczegółowego śledzenia zmian wprowadzanych przez różnych operatorów i administratorów systemu.
2. Zapis zmian powinien odbywać się w zewnętrznej bazie danych a dostęp powinien być realizowany przez zewnętrzne narzędzie, niezagrzeżdżone w interfejsie klienta.

#### **Wykorzystanie skryptów**

1. System zarządzania wideo oferuje wbudowany edytor skryptów poleceń, umożliwiający napisanie własnych skryptów do wirtualnego sterowania funkcjami systemu. Skrypty poleceń mogą być uruchamiane przez operatorów lub automatycznie, w odpowiedzi na zdarzenia alarmowe lub systemowe. Wbudowany edytor skryptów poleceń wspiera języki C# oraz VB.NET.
2. System jest konfigurowalny w taki sposób, że operatorzy mogą wykonywać stworzone skrypty przez podwójne kliknięcie na odpowiednich ikonach w drzewie logicznym lub na mapie lokalizacji.
3. System umożliwia konfigurację w taki sposób, że stworzone skrypty są wykonywane automatycznie w odpowiedzi na zdarzenia systemowe. Automatyczne wykonywanie skryptów może być opcjonalnie ograniczone harmonogramami.
4. System umożliwia wykonanie skryptów poleceń dla danej grupy użytkowników w momencie zalogowania użytkownika do systemu.
5. System umożliwia wykonanie skryptów poleceń dla alarmów w momencie zaakceptowania alarmu przez operatora.
6. W ramach wykorzystania skryptów system zarządzania wideo powinien umożliwiać wystawianie wgranych w głośnik IP komunikatów ostrzegawczych.
  - a. Wyzwolenie komunikatu powinno móc odbywać się z przycisku zdefiniowanego przez administratora.

- b. Wyzwolenie komunikatu powinno móc odbywać się w odpowiedzi na dowolne zdarzenie i alarm odbierane przez system zarządzania.

#### **Infrastruktura IT**

1. Podgląd obrazu z kamer jest możliwy na jednej lub wielu stacjach roboczych jednocześnie. Kamery, rejestratory i stacje robocze mogą być umieszczone w dowolnym miejscu w sieci IP.
2. System zarządzania wspiera protokół LDAP, umożliwiający integrację z systemami zarządzania użytkownikami, jak Microsoft Active Directory.
3. Oprogramowanie serwera zarządzającego umożliwia zarządzanie, monitorowanie i kontrolę pracy całego systemu.
4. Oprogramowanie powinno być przetestowane z rozwiązaniami wirtualizacji lub wysokiej dostępności, takimi jak Vmware vSphere, Microsoft HyperV oraz Stratus Everrun.
5. System zarządzania umożliwia monitorowanie urządzeń poprzez protokół SNMP (co najmniej SNMPv2).

#### **Integracja z systemami zewnętrznymi**

1. System zarządzania wideo umożliwia integrację z:
  - a. Systemami rozpoznawania twarzy
  - b. Naziemnymi systemami detekcji radarowej
  - c. Systemami ochrony perymetrycznej
  - d. Systemami zarządzania bezpieczeństwem fizycznym
  - e. Systemami rozpoznawania tablic rejestracyjnych
2. System zarządzania wideo powinien umożliwiać uruchomienie zdarzenia alarmowego, na podstawie informacji otrzymanej z tego typu systemów.
3. System zarządzania wideo umożliwia modyfikację, z wykorzystaniem SDK, tak, aby:
  - a. weryfikować alarm z innych systemów (baz danych) przed zaprezentowaniem operatorowi.
  - b. przesyłać informacje do innych systemów z wykorzystaniem dedykowanych protokołów.
4. Dla systemu zarządzania wideo dostępne są udokumentowane biblioteki SDK (Software Development Kit), umożliwiające integrację z oprogramowaniem firm trzecich.
5. Funkcjonalności SDK wymagają autentykacji w systemie.
6. Biblioteki SDK są dostępne dla wszystkich języków programowania .Net.
7. System zarządzania wideo posiada wbudowany serwer OPC do integracji z oprogramowaniem zewnętrznym, takim jak systemy BMS, SMS, czy PSIM.
8. Interfejs OPC obsługuje standard OPC Alarms and Events.
9. Możliwość zagnieżdżenia w widoku urządzeń linków do zewnętrznych aplikacji.
10. Możliwość wykorzystania REST API oferowane przez producenta.

#### **Obsługa inteligentnej analizy obrazu i analizy dźwięku**

1. System zarządzania wideo umożliwia konfigurację parametrów inteligentnej analizy obrazu w urządzeniu końcowym z poziomu interfejsu konfiguracyjnego.
2. System będzie reagował na zdarzenia, wywołane funkcjami inteligentnej analizy obrazu w urządzeniu końcowym, w tym w kamerze IP lub enkoderze.
3. Wszystkie zdarzenia są zapisywane w dzienniku zdarzeń, umożliwiając późniejsze przeszukiwanie.
4. Metadane, generowane przez urządzenia końcowe, są zapisywane wraz z nagraniami, co umożliwia operatorowi szybkie przeszukiwanie nagrań pod kątem określonych zdarzeń również wtedy, gdy alarmy inteligentnej analizy obrazu nie zostały uprzednio skonfigurowane w kamerze.
5. Aplikacja kliencka umożliwia operatorowi podgląd reguł alarmowych, skonfigurowanych w kamerach z funkcją inteligentnej analizy obrazu.
6. System zarządzania wideo umożliwia integrację z funkcjami inteligentnej analizy dźwięku realizowanej w urządzeniu końcowym.
  - a. System odbiera informacje o typie dźwięku: wystrzał z broni, alarm T1 i T2
  - b. Urządzenie końcowe wyposażone w co najmniej 3 mikrofony wysokoczułe powinno mieć możliwość podawania przybliżonego kierunku pochodzenia dźwięku.

#### **Bezpieczeństwo systemu**

1. System zarządzania wideo umożliwia stworzenie grup użytkowników z uprawnieniami do dostępu do określonych kamer, priorytetem sterowania PTZ, uprawnieniami eksportowania nagrań oraz dostępu do dziennika zdarzeń systemowych. Dostęp do podglądu na żywo, nagrań wideo, audio, sterowania PTZ, wywoływania położeń zaprogramowanych i poleceń pomocniczych może być programowany na poziomie pojedynczej kamery w systemie.
2. Aby ograniczyć potencjalne ryzyko ataku typu „brute-force”, system nie może posiadać niemodyfikowalnego konta o uprawnieniach administratora.
3. System zarządzania umożliwia stworzenie grup użytkowników, gdzie wymagane jest uwierzytelnianie dwupoziomowe.
4. System zarządzania wideo umożliwia potwierdzenie autentyczności zarejestrowanych nagrań. Wspierane jest sprawdzenie wartości sumy kontrolnej względem danych wideo z kamer, które dostarczają strumień do rejestracji z wartościami sumy kontrolnej, podpisanymi certyfikatem.
5. Oprogramowanie klienckie umożliwia wylogowanie bezpieczeństwa po upływie określonego czasu bezczynności
  - a. Aplikacja kliencka zostanie wylogowana automatycznie, gdy przez dany okres czasu nie zostanie wykryta aktywność operatora
6. Możliwe jest wymuszenie polityki bezpieczeństwa haseł logowania do aplikacji klienckiej przez użytkowników.
  - a. Gdy uruchomione zostanie wymuszenie ustanowienia bezpiecznego hasła, aplikacja kliencka będzie akceptować jedynie hasła:
    - i. o długości co najmniej 8 znaków
    - ii. z przynajmniej jedną literą małą
    - iii. z przynajmniej jedną literą wielką
7. Możliwe jest zablokowanie konta po określonej, konfigurowalnej liczbie nieudanych prób logowania.
8. Możliwe jest skonfigurowanie maksymalnego czasu obowiązywania hasła.
9. Możliwa jest dezaktywacja konta użytkownika.
10. Możliwe jest wymuszenie zmiany hasła użytkownika przy kolejnym logowaniu.
11. System zarządzania wideo umożliwia stworzenie grup użytkowników, mających uprawnienia dostępu do poszczególnych funkcji konfiguracyjnych, z podziałem na co najmniej: urządzenia, mapy i drzewo logiczne, harmonogramy, parametry rejestracji, zdarzenia, alarmy i grupy użytkowników.
12. System zarządzania umożliwia skonfigurowanie danych uwierzytelniających dostęp do zewnętrznych zasobów sieciowych (aplikacji zagnieżdżonych), aby nie zachodziła potrzeba ręcznego logowania do tych zasobów przez operatora.
13. Możliwe jest skonfigurowanie bezpiecznej, szyfrowanej komunikacji pomiędzy serwerem zarządzającym a kamerami oraz pomiędzy aplikacją kliencką a kamerami
  - a. Aplikacja kliencka umożliwia dekodowanie obrazu z zabezpieczonego (AES-128) strumienia multi-cast
  - b. Aplikacja kliencka umożliwia dekodowanie obrazu z zabezpieczonego (AES-256) strumienia uni-cast
14. System umożliwia szyfrowanie rejestrowanych danych poprzez AES-256 bez spadku wydajności (liczby obsługiwanych kamer i przepustowości) rejestratora.
15. System zarządzający umożliwia odtwarzanie nagrań wideo, zaszyfrowanych poprzez AES-256.

#### **Zapewnienie zgodności**

1. System zarządzania wideo jest wyspecyfikowany jako produkt zgodny z ONVIF Profile-S na witrynie internetowej organizacji ONVIF.
2. Funkcjonalność skanowania umożliwia wykrycie kamer zgodnych z ONVIF Profile-S
3. Z poziomu systemu zarządzania wideo możliwa jest podstawowa konfiguracja kamer zgodnych z ONVIF Profile-S, jak ogólne ustawienia kamery (np. strumieniowanie multicast), profile rejestracji (kodek, rozdzielczość, liczba klatek na sekundę) i profile audio.
4. Możliwe jest wykorzystanie zdarzeń z kamer ONVIF Profile-S do wyzwalania zdarzeń i alarmów w systemie.
5. System powinien umożliwiać podłączenie kamer i/lub innych źródeł sygnału wizyjnego za pośrednictwem strumienia RTSP.

#### **Konfiguracja**

1. System zarządzania wideo oferuje zintegrowany interfejs do konfiguracji i zarządzania systemem.

2. System umożliwia skonfigurowanie domyślnie wyświetlanego strumienia z kamery względem określonej stacji roboczej i/lub względem danej kamery.
3. Profile użytkowników, wraz z poszczególnymi ustawieniami są przechowywane centralnie, na serwerze. Ustawienia te są dostępne dla danego użytkownika niezależnie od fizycznej stacji roboczej, z której w danej chwili on korzysta.
4. Zmiany, wprowadzane w konfiguracji systemu zarządzania wideo, będą wprowadzane w kopii roboczej aktualnej konfiguracji i nie będą bezpośrednio wpływały na aktywną i wykorzystywaną w danej chwili konfigurację systemu.
5. Oprogramowanie konfiguracyjne umożliwia w dowolnym momencie aktywowanie kopii roboczej ustawień tak, aby stała się ona aktywną i wykorzystywaną konfiguracją systemu.
6. Możliwe jest ustalenie przyszłej daty i godziny, o której dana kopia konfiguracji stanie się aktywna.
7. Aplikacja daje operatorowi możliwość lokalnej aktywacji nowej konfiguracji natychmiast lub odłożenia tego procesu w czasie. Możliwe jest również wymuszenie aktywacji nowej konfiguracji dla wszystkich aplikacji klienckich w obrębie danego serwera.
8. System zarządzania wideo udostępnia do 10 różnych i niezależnych harmonogramów nagrywania. Mogą one być wykorzystane do zapewnienia zmiennej liczby klatek na sekundę w ciągu dnia, nocy, czy dni wolnych i świątecznych. Harmonogramy mogą być również wykorzystane do umożliwienia logowania określonej grupie użytkowników, wyzwalania alarmów przez określone zdarzenia, czy eksportowania nagrań.
9. System daje możliwość odtwarzania nagrań, wyeksportowanych w formacie natywnym, bez potrzeby instalowania dedykowanej aplikacji na stacji klienckiej.

### **Zgodność z normami**

1. Produkt musi pochodzić od firmy, spełniającej wymagania systemu zarządzania jakością ISO-9001 oraz EN-29001.
2. System zarządzania wideo powinien umożliwiać taką konfigurację, aby była możliwość zapewnienia zgodności z wymaganiami normy IEC 62676.
  - a. Konfiguracja systemu zarządzania musi umożliwiać konfigurację systemu zgodnie z wymaganiami stawianymi w grade 4.
  - b. Spełnienie wymagań Grade 4 powinno być poparte dokumentem technicznym opisującym w jakim stopniu i przy jakich ustawieniach jest ten poziom spełniony.
3. System zarządzania wideo powinien umożliwiać taką konfigurację, aby zapewniona została zgodność z wymaganiami RODO danej organizacji.

### **Kamera kopułkowa**

Opis funkcjonalny:

Do dozoru przestrzeni wewnętrznych planuje się wykorzystanie kamer typu Turret, o rozdzielczości FullHD. Kamera charakteryzuje się szerokim zakresem dynamiki 120dB, oferując wysoką jakość obrazu przy wymagających warunkach oświetleniowych. Zintegrowany obiektyw z ogniskową 2,3 mm oferuje szeroki kąt obserwacji 130°. Kamery wyposażone są w zintegrowany oświetlacz podczerwieni o zasięgu 15 metrów i cechują się konstrukcją, minimalizującą odbicia światła.

W celu zapewnienia optymalnej efektywności systemu przy ograniczonej liczbie operatorów przyjmuje się aktywne wykorzystanie mechanizmów zaawansowanej analizy obrazów dla kamer CCTV. Tym samym wszystkie kamery w systemie będą fabrycznie wyposażone w funkcje inteligentnej analizy obrazu – nie wymaga to zakupu i uruchamiania dodatkowych licencji. Analiza obrazu odbywa się bezpośrednio w kamerze, dzięki czemu zapewniona jest najwyższa skuteczność (praca na nieskompresowanym obrazie) oraz skalowalność. W kamerach planuje się skonfigurowanie algorytmów analizy, umożliwiających:

- Wykrycie obecności osób w strefie, w celu skutecznej ochrony przeciwwłamaniowej;
- Zliczanie osób wchodzących, wychodzących lub przemieszczających się po obiekcie;
- Nienaturalne szwędanie się osób w wyznaczonych obszarach;
- Pozostawienie podejrzanego obiektu czy zastawienie wyjścia ewakuacyjnego;

- Wykrycie sytuacji nietypowych, jak stan paniki.

W celu znacznie skuteczniejszego wykorzystania funkcji inteligentnej analizy obrazu, kamera będzie w stanie automatycznie sklasyfikować rozpoznany obiekt (jako człowieka, rowerzystę, samochód osobowy lub samochód ciężarowy). Rodzaj obiektu będzie wskazany na obrazie poprzez wyświetlanie odpowiedniej ikonki, obok dokładnego obrysu obiektu. W ten sposób, każda ze skonfigurowanych funkcji może reagować jedynie na dany rodzaj obiektu, co minimalizuje liczbę fałszywych alarmów.

Kamera jest w stanie w sposób automatyczny zmieniać parametry wszystkich strumieni wizyjnych, w zależności od określonego harmonogramu lub wystąpienia stanu alarmowego. Ponadto, kamera umożliwia zapisywanie skryptów, w celu tworzenia odpowiednich zależności logicznych i rozbudowanych reakcji na alarmy, bezpośrednio w kamerze.

Celem zwiększenia efektywności i znacznego skrócenia czasu przeszukiwania nagrań przez operatorów, mechanizmy inteligentnej analizy obrazów wykorzystywane będą również do analizy wstecznej. Przeszukiwanie nagrań odbywać się powinno na podstawie zgromadzonych metadanych. Operator definiuje parametry w momencie wyszukiwania określonego zdarzenia, niezależnie od wcześniej skonfigurowanych w kamerze alarmów. W ten sposób możliwe jest przeszukanie nagrań pod kątem zdarzeń takich, jak:

- Pojawienia się w scenie lub w określonej strefie obiektów sklasyfikowanych jako człowiek;
- Określenia kierunku poruszania się osoby;
- Określenia koloru ubioru osoby;

Istotną kwestią będzie także cyberbezpieczeństwo całego układu sieciowego i wszystkich systemów security bazujących na nim. Zakłada się szyfrowaną komunikację pomiędzy kamerami, serwerem zarządzającym, stacjami operatorskimi i systemem zapisu, przy wykorzystaniu algorytmów szyfrujących AES z kluczem 256 bit. Kamera powinna wspierać uwierzytelnianie zgodnie ze standardem 802.1x oraz protokół TLS 1.2.

Kamera daje możliwość obsługi kart MicroSD o pojemności do 2 TB. W przypadku zastosowania kart w wykonaniu przemysłowym kamera może monitorować aktualny stan karty i automatycznie alarmować, w przypadku przekroczenia określonego limitu jej żywotności.

Kamera daje możliwość zapisania danych geolokacyjnych – na temat dokładnych współrzędnych jej położenia – co przy zastosowaniu odpowiedniego oprogramowania umożliwia dokładne umiejscowienie kamery na mapie i oznaczenie na mapie wykrytych obiektów.

Kamera daje możliwość skonfigurowania do 8 masek prywatności. Aby zapewnić odpowiednią czytelność obrazu dostępne są do wyboru 3 kolory masek, w tym maska zlewająca się z kolorem tła.

Wymagania techniczne:

Parametr	Wymagania minimalne
Budowa	Kamera kopułkowa płaska
Rozdzielczość	1920x1080 @ 30fps
Przetwornik	CMOS 1/2,8"
Czułość	Nie gorsza niż 0,1 lux w trybie dziennym i 0,02 lux w trybie nocnym zgodnie z IEC 62676 Część 5 (1/30, F1.6 lub F2.2). 0,0 lux przy włączonym oświetlaczu IR
Zakres dynamiki	120 dB
Kompresja	H.265; H.264; M- JPEG
Obszary ROI	Do 8 obszarów z niezależnymi ustawieniami jakości kodowania

Stosunek sygnał/szum	>55 dB
Migawka	Tryby migawki: automatyczna, wybierana ręcznie.
Obiektyw	Zintegrowany 2,3 mm
Kąt obserwacji	132° x 77°
Oświetlacz IR	Zintegrowany o zasięgu co najmniej 15 m
Obsługiwane protokoły	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP, FTP, ARP, DHCP, APIPA (Auto-IP, link local address), NTP (SNTP), SNMP (V1, V3, MIB-II), 802.1x, DNS, DNSv6, DDNS, SMTP, iSCSI, UPnP (SSDP), DiffServ (QoS), LLDP, SOAP, Dropbox™, CHAP, digest authentication
Bezpieczeństwo danych	<p>Wsparcie uwierzytelnienia poprzez protokół EAP-TLS 1.2 także z możliwością wgrania certyfikatu w zakresie infrastruktury klucza publicznego do szyfrowania cyfrowego dostarczonego przez producenta kamery, tworzonego przez użytkownika oraz certyfikowane rozwiązania firm 3-ch</p> <p>Wsparcie szyfrowania na poziomie sprzętowym tj fabrycznie zabudowany moduł TPM (Trusted Platform Module), który wykorzystuje klucz kryptograficzny do ochrony wszystkich zarejestrowanych danych</p>
Autentykacja wideo	Znak wodny, SHA-1, SHA-256
Łącze sieciowe	RJ-45 100 Base-TX Ethernet
Strumień wideo	Możliwość generowania 4 strumieni wideo
Inteligentna analiza obrazów	<p>Wbudowana w kamerę z możliwością równoległej analizy do 16 reguł alarmowych</p> <p>Analizowane algorytmy:</p> <ul style="list-style-type: none"> <li>• wykrycie obiektu</li> <li>• przekroczenie linii</li> <li>• kierunkowość ruchu</li> <li>• porzucenie obiektu</li> <li>• zmiana stanu obiektu</li> <li>• gęstość tłumy</li> <li>• zliczanie – przekroczenie linii</li> <li>• zliczanie obiektów w określonych strefach</li> </ul> <p>Zaawansowane funkcje w zakresie kalibracji i monitorowania obiektu takie jak np. ustalone proporcje obiektu, kolor obiektu oraz kierunek i prędkość jego przemieszczania</p> <p>Możliwość prezentowania statystyki dla wybranego pola lub obiektu z możliwością odczytu rzeczywistych wartości takich jak prędkości obiektu, jego proporcje i kolor czy kierunek jego poruszania</p> <p>Możliwość analizy materiału zarejestrowanego na podstawie metadanych</p>
Zapis lokalny	Wbudowany slot karty SD/microSD (obsługa kart do 2 TB), wsparcie kart SD w wykonaniu przemysłowym z monitorowaniem stanu żywotności karty SD
Pre-alarm	5s
Zgodność	ONVIF Profile S, Profile G, Profile T
Wejście alarmowe	1
Wyjście przekaźnikowe	1
Wejście audio	Wbudowany mikrofon
Wyjście audio	1
Alarm audio	Alarm na podstawie wykrycia dźwięku
Maski prywatności	8
Temperatura pracy	-20 - +50 °C
Stopień ochrony mechanicznej	IK08
Zasilanie	Sieciowe lub PoE
Gwarancja	5 lat

Kamera bullet

Opis funkcjonalny:

Do dozoru przestrzeni zewnętrznych planuje się wykorzystanie kamer wandaloodpornych typu „bullet”, o rozdzielczości 5 Mpx. Dla zapewnienia wysokiej jakości i szczegółowości obrazu również w ciemności, kamera posiada wbudowany oświetlacz podczerwieni o zasięgu 30m. Zintegrowany obiektyw z możliwością zdalnej regulacji ogniskowej daje możliwość łatwego dopasowania obserwowanej sceny oraz automatycznego wyostrenia obrazu z kamery.

W celu zapewnienia optymalnej efektywności systemu przy ograniczonej liczbie operatorów przyjmuje się aktywne wykorzystanie mechanizmów zaawansowanej analizy obrazów dla kamer CCTV. Tym samym wszystkie kamery w systemie będą fabrycznie wyposażone w funkcje inteligentnej analizy obrazu – nie wymaga to zakupu i uruchamiania dodatkowych licencji. Analiza obrazu odbywa się bezpośrednio w kamerze, dzięki czemu zapewniona jest najwyższa skuteczność (praca na nieskompresowanym obrazie) oraz skalowalność. W kamerach planuje się skonfigurowanie algorytmów analizy, umożliwiających:

- Wykrycie obecności osób w strefie, w celu skutecznej ochrony przeciwwłamaniowej;
- Parkowanie pojazdu w niedozwolonym miejscu lub dłużej, niż dopuszczalne;
- Zliczanie osób wchodzących, wychodzących lub przemieszczających się po obiekcie;
- Nienaturalne szwędanie się osób w wyznaczonych obszarach;
- Pozostawienie podejrzanego obiektu czy zastawienie wyjścia ewakuacyjnego;
- Wykrycie sytuacji nietypowych, jak stan paniki.

W celu znacznie skuteczniejszego wykorzystania funkcji inteligentnej analizy obrazu, kamera będzie w stanie automatycznie sklasyfikować rozpoznany obiekt (jako człowieka, rowerzystę, samochód osobowy lub samochód ciężarowy). Rodzaj obiektu będzie wskazany na obrazie poprzez wyświetlanie odpowiedniej ikonki, obok dokładnego obrysu obiektu. W ten sposób, każda ze skonfigurowanych funkcji może reagować jedynie na dany rodzaj obiektu, co minimalizuje liczbę fałszywych alarmów.

Kamera jest w stanie w sposób automatyczny zmieniać parametry wszystkich strumieni wizyjnych, w zależności od określonego harmonogramu lub wystąpienia stanu alarmowego. Ponadto, kamera umożliwia zapisywanie skryptów, w celu tworzenia odpowiednich zależności logicznych i rozbudowanych reakcji na alarmy, bezpośrednio w kamerze.

Celem zwiększenia efektywności i znacznego skrócenia czasu przeszukiwania nagrań przez operatorów, mechanizmy inteligentnej analizy obrazów wykorzystywane będą również do analizy wstecznej. Przeszukiwanie nagrań odbywać się powinno na podstawie zgromadzonych metadanych. Operator definiuje parametry w momencie wyszukiwania określonego zdarzenia, niezależnie od wcześniej skonfigurowanych w kamerze alarmów. W ten sposób możliwe jest przeszukanie nagrań pod kątem zdarzeń takich, jak:

- Pojawienia się w scenie lub w określonej strefie obiektów sklasyfikowanych jako człowiek;
- Określenia kierunku poruszania się osoby;
- Określenia koloru ubioru osoby lub koloru pojazdu;

Istotną kwestią będzie także cyberbezpieczeństwo całego układu sieciowego i wszystkich systemów security bazujących na nim. Zakłada się szyfrowaną komunikację pomiędzy kamerami, serwerem zarządzającym, stacjami operatorskimi i systemem zapisu, przy wykorzystaniu algorytmów szyfrujących AES z kluczem 256 bit. Kamera powinna wspierać uwierzytelnianie zgodnie ze standardem 802.1x oraz protokół TLS 1.2.

Kamera daje możliwość obsługi kart MicroSD o pojemności do 2 TB. W przypadku zastosowania kart w wykonaniu przemysłowym kamera może monitorować aktualny stan karty i automatycznie alarmować, w przypadku przekroczenia określonego limitu jej żywotności.

Kamera daje możliwość zapisania danych geolokacyjnych – na temat dokładnych współrzędnych jej położenia – co przy zastosowaniu odpowiedniego oprogramowania umożliwia dokładne umiejscowienie kamery na mapie i oznaczenie na mapie wykrytych obiektów.

Kamera daje możliwość skonfigurowania do 8 masek prywatności. Aby zapewnić odpowiednią czytelność obrazu dostępne są do wyboru 3 kolory masek, w tym maska zlewająca się z kolorem tła.

Wymagania techniczne:

Parametr	Wymagania minimalne
Budowa	Kamera w obudowie zintegrowanej typu "bullet"
Rozdzielczość	3072x1728 @ 20fps; 2720x1530 @ 25fps
Przetwornik	CMOS 1/2,9"
Czułość	Nie gorsza niż 0,379 lux w trybie dziennym i 0,042 lux w trybie nocnym zgodnie z IEC 62676 Część 5 (1/30, F1.6) 0,0 lux przy włączonym oświetlaczu IR
Zakres dynamiki	120 dB
Kompresja	H.265; H.264; M- JPEG
Obszary ROI	Do 8 obszarów z niezależnymi ustawieniami jakości kodowania
Stosunek sygnał/szum	>55 dB
Migawka	Tryby migawki: automatyczna, wybierana ręcznie.
Oświetlacz IR	Wbudowany, o zasięgu 30 m, z regulacją intensywności
Obiektyw	Zintegrowany 3,2 - 10 mm ze zdalną regulacją zoom i autofocusem
Obsługiwane protokoły	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP, FTP, ARP, DHCP, APIPA (Auto-IP, link local address), NTP (SNTP), SNMP (V1, V3, MIB-II), 802.1x, DNS, DNSv6, DDNS, SMTP, iSCSI, UPnP (SSDP), DiffServ (QoS), LLDP, SOAP, Dropbox™, CHAP, digest authentication
Bezpieczeństwo danych	Wsparcie uwierzytelnienia poprzez protokół EAP-TLS 1.2 także z możliwością wgrania certyfikatu w zakresie infrastruktury klucza publicznego do szyfrowania cyfrowego dostarczonego przez producenta kamery, tworzonego przez użytkownika oraz certyfikowane rozwiązania firm 3-ch Wsparcie szyfrowania na poziomie sprzętowym tj fabrycznie zabudowany moduł TPM (Trusted Platform Module), który wykorzystuje klucz kryptograficzny do ochrony wszystkich zarejestrowanych danych
Autentykacja wideo	Znak wodny, SHA-1, SHA-256
Łącze sieciowe	RJ-45 100 Base-TX Ethernet
Strumień wideo	Możliwość generowania 4 strumieni wideo
Inteligentna analiza obrazów	Wbudowana w kamerę z możliwością równoległej analizy do 16 reguł alarmowych Analizowane algorytmy: <ul style="list-style-type: none"> <li>• wykrycie obiektu</li> <li>• przekroczenie linii</li> <li>• kierunkowość ruchu</li> <li>• porzucenie obiektu</li> <li>• zmiana stanu obiektu</li> <li>• gęstość tłumy</li> <li>• zliczanie – przekroczenie linii</li> <li>• zliczanie obiektów w określonych strefach</li> </ul> Zaawansowane funkcje w zakresie kalibracji i monitorowania obiektu takie jak np. ustalone proporcje obiektu, kolor obiektu oraz kierunek i prędkość jego przemieszczania Możliwość prezentowania statystyki dla wybranego pola lub obiektu z możliwością odczytu rzeczywistych wartości takich jak prędkości obiektu, jego proporcje i kolor czy kierunek jego poruszania

	Możliwość analizy materiału zarejestrowanego na podstawie metadanych
Zapis lokalny	Wbudowany slot karty SD/microSD (obsługa kart do 2 TB), wsparcie kart SD w wykonaniu przemysłowym z monitorowaniem stanu żywotności karty SD
Pre-alarm	5s
Zgodność	ONVIF Profile S, Profile G, Profile T
Wejście alarmowe	1
Wyjście przekaźnikowe	1
Wejście audio	1
Wyjście audio	1
Alarm audio	Alarm na podstawie wykrycia dźwięku
Maski prywatności	8
Temperatura pracy	-30 - +50 °C
Stopień ochrony	IP66
Wandaloodporność	IK10
Zasilanie	Sieciowe lub PoE
Gwarancja	5 lat

## MONTAŻ URZĄDZEŃ

Dokładne rozmieszczenie urządzeń zostało pokazane na planie instalacji CCTV.

Wszystkie elementy instalacji powinny być oznaczone alfanumerycznie, w sposób trwały. Nie dopuszcza się oznaczeń w postaci pisania na powłokach kablowych, należy stosować specjalne trwałe oznaczniki. Te same oznaczenia powinny być użyte w urządzeniach monitorujących, sterujących, wizualizujących system oraz w dokumentacji powykonawczej.

Przewody należy instalować tak, aby chronić je przed uszkodzeniami w rurkach ochronnych możliwie z dala od instalacji mogących mieć wpływ na funkcjonowanie systemu. Przejścia przewodów instalacji przez ściany zewnętrzne oraz wewnętrzne pomiędzy strefami pożarowymi uszczelnić przy pomocy mas uszczelniających o odporności właściwej dla ścian, które są uszczelniane.

Montaż wszystkich urządzeń wykonać zgodnie z DTR poszczególnych urządzeń oraz według wytycznych producenta.

## ZALECENIA URUCHAMIANIA, EKSPLOATACJI I KONSERWACJI

Przed przekazaniem systemu do eksploatacji zaleca się dokładne sprawdzenie systemu i przeprowadzenie prób funkcjonalnych oraz przeprowadzenie pomiarów sprawdzających wszystkich łączy. Należy również wykonać dokumentację powykonawczą oraz przeszkolić pracowników obsługujących system.

### Zestawienie podstawowych materiałów:

Lp.	Opis	Ilość
1.	Kamera kopułkowa IP, 1080p, h.265, f=2,3mm, IR 15m, IK08, WDR 120dB, analityka EVA, slot microSD, iDNR, Intelligent Streaming, szyfrowanie AES256, Onvif Profile S, G, T	25
2.	Kamera IP bullet, 5MP, h.265, AVF 3,2-10mm, IR 30m, IK10, IP66. WDR 120dB, analityka EVA, slot microSD, iDNR, Intelligent Streaming, szyfrowanie AES256, Onvif Profile S, G, T	13
3.	Uchwyt ścienny do montażu zwisowego	1
4.	Rejestrator IP dysk 4x8TB, 1U, 3 tryby pracy: BVMS (wymagana licencja MBV-BPLU-DIP), VRM, target iSCSI, rozbudowa do max. 64 kanałów, przepustowość 400Mb/s, RAID5 / RAID5+HotSpare / RAID6	1
5.	Rejestrator IP - Licencja podstawowa Plus, zawiera 32 kanały BVMS (max. 64), 5 stacji roboczych (max. 10), 1 DVR (max. 10), 5 klawiatur (max. 10), 1 centralę B/G (max. 10), 1	1

	usługę MVS (max. 4), ATM/POS, OPC	
6.	Dla obu wersji DIP all-in-one (rozbudowa o <b>1 kanał</b> )	6
7.	Ogranicznik przepięć PoE	13
8.	Ogranicznik przepięć 16 kanałów sieci LAN / IP-CCTV,	1
9.	Switch 48 x 10/100/1000 (PoE+) + 4 x Gigabit SFP, 760W PoE	1

## 19. INSTALACJA SYGNALIZACJI WŁAMANIA I NAPADU

### Podstawowe funkcje systemu SSWiN

Zakłada się zaprojektowanie systemu sygnalizacji włamania i napadu zgodnego z normą EN 50131 stopnia 3, co oznacza, że centrala i jej podzespoły są przeznaczone dla instalacji o średnim lub wysokim stopniu ryzyka.

Centrala ma za zadanie chronić przed potencjalnym intruzem, który może posiadać dobrą wiedzę na temat systemów alarmowych, oraz może mieć dostęp do specjalistycznych narzędzi służących do rozbrojenia / zakłócenia działania systemu. Dlatego też ważne, aby jak najwięcej elementów końcowych systemu, takich jak różnego rodzaju moduły i detektory były również przebadane na zgodność z normą EN 50131 i posiadały stopień 3.

System powinien być budowany w oparciu o moduły. Dzięki tej funkcjonalności będzie możliwe tworzenie elastycznych systemów, których rozmiar i rozproszenie będzie determinowane przez rodzaj i ilość wybranych modułów operacyjnych. Połączenie pomiędzy modułami powinno być realizowane za pomocą magistrali komunikacyjnej pozwalającej na oddalenie ostatniego elementu nawet o 1000 m od panelu głównego centrali alarmowej.

System powinien oferować moduł służący do rozdzielania magistrali zewnętrznej, dzięki czemu możliwe będzie tworzenie do dwóch odgałęzień po 500 m każde.

System powinien umożliwiać w przyszłości rozbudowę polegającą na dodawaniu kolejnych modułów lub czujników.

Konfiguracja systemu powinna odbywać się za pomocą darmowego oprogramowania dostarczanego od producenta systemu.

System powinien umożliwiać integrację z innymi systemami bezpieczeństwa pod jedną wspólną platformą służącą do nadzoru i integracji. Integracja z innymi systemami i przekazywanie informacji

o stanach stref i urządzeń powinny się odbywać za pomocą otwartego protokołu komunikacyjnego, możliwego do czytania również przez obce systemy typu SMS.

Aplikacja obsługująca otwarty protokół komunikacyjny powinna być dostarczana przez dostawcę nieodpłatnie z każdą z wersji oprogramowania do konfiguracji.

Powinna istnieć możliwość integracji kilku systemów sygnalizacji włamania i napadu i wizualizacji ich jako jednego wspólnego.

Połączenie central powinno wymagać jak najmniejszej ilości fizycznych połączeń i ograniczyć się do włączenia central do wspólnej sieci z oprogramowaniem nadrzędnym rodzimego lub obcego dostawcy.

System sygnalizacji włamania i napadu powinien umożliwiać integrację min. z kontrolą dostępu, systemem sygnalizacji pożaru, dźwiękowym systemem ostrzegawczym oraz systemem telewizji dozorowej.

System integrujący (zwany również nadrzędnym) powinien umożliwiać operatorowi dostęp do treści skonfigurowanych w pojedynczej centrali lub układzie składającym się z wielu central. Operator systemu integrującego powinien mieć dostęp do skonfigurowanych dla siebie treści. Centrala alarmowa powinna mieć możliwość (w przypadku konieczności) odłączenia się od systemu integrującego, lub pozostawienie jedynie podglądu swoich stanów bez możliwości nadrzędnej kontroli nad systemem.

System powinien umożliwiać również fizyczną integrację z innymi systemami, np. z systemem kontroli dostępu poprzez połączenie przewodowe wejść i wyjść centrali i kontrolera KD i przekazywanie między systemami informacji na temat stanów skonfigurowanych stref i urządzeń. Dzięki tej funkcjonalności zapewnione będzie np. rozbrajanie i uzbrajanie stref systemu za pomocą dedykowanych czytników do systemu KD.

Pojedynczy system sygnalizacji włamania i napadu powinien być w stanie obsłużyć łącznie do 1500 elementów wchodzących w skład detekcji rozumianych jako wejścia i wyjścia fizycznie (łącznie ponad 1000 na jeden system) oraz wejścia i wyjścia wirtualne.

System powinien umożliwiać również podzielenie wszystkich skonfigurowanych i podłączonych elementów na 500 stref, które mogą pozostawać wobec siebie niezależne. Użytkownik systemu będzie w stanie tworzyć relacje pomiędzy strefami polegające na tworzeniu stref nadrzędnych, podrzędnych, bocznych, przejściowych i innych, mając równoczesną możliwość korzystania z gotowych scenariuszy, a także tworzenia swoich własnych dotyczących zachowań międzystrefowych przy użyciu wirtualnych wejść i wyjść.

Zakłada się, że system będzie w stanie obsługiwać nawet do 1000 użytkowników. System powinien umożliwiać zadeklarowanie treści i działań, które dany użytkownik będzie w stanie widzieć lub wykonywać po zalogowaniu się do systemu.

Projektowany system powinien być w stanie tworzyć grupy użytkowników i konfigurację dla nich wielu cech wspólnych, między innymi praw dostępu do operacji, konserwacji czy uzbrajania i rozbrajania stref. Użytkownik powinien za pomocą manipulatora wykonać jedynie operacje, które zostaną mu wcześniej zadeklarowane.

Panel główny systemu sygnalizacji włamania i napadu jako element główny powinien zapewniać dodatkowo do 8 nadzorowanych wejść do podłączenia urządzeń, wejście antysabotażowe, 4 programowalne wyjścia (w tym dwa przekaźnikowe) i wyjście zasilania dodatkowego. Panel główny powinien posiadać wbudowane złącze Ethernet służące do konfiguracji całego systemu. Wbudowane złącze Ethernet powinno być jedynym elementem służącym do podłączenia systemu do wspólnej platformy integrującej.

Pojedynczy system sygnalizacji włamania i napadu powinien umożliwiać obsługę do 32 manipulatorów dotykowych.

Manipulator powinien zapewniać użytkownikowi zakres wyświetlanych treści zależny od skonfigurowanych wcześniej dla niego praw.

Projektowany manipulator powinien posiadać wskaźniki diodowe mogące indykować aktualny status działania systemu z uwzględnieniem pracy normalnej, problemu natury technicznej i alarmu.

Manipulator systemu powinien umożliwiać (w zależności od praw zalogowanego użytkownika) pełną kontrolę nad działaniem systemu obejmującą działania operacyjne, konserwacyjne, monitorujące i inne.

Projektowany manipulator powinien być w stanie obsługiwać wiele popularnych języków. Treść zalogowanego użytkownika powinna wyświetlać się w zadeklarowanym dla niego języku (Niemiecki, Angielski, Francuski, Holenderski, Węgierski, Polski, Włoski, Rosyjski, Hiszpański, Czeski, Portugalski, Łotewski).

System powinien dysponować klawiaturą strefową służącą do uzbrajania i rozbrajania strefy lokalnej. W zależności od konfiguracji elementu podłączeniowego system jednocześnie powinien być w stanie oferować:

- Blokowanie drzwi,
- Monitorowanie rygla,
- Monitorowanie otwarcia/zamknięcia drzwi za pomocą kontaktronu konwencjonalnego,
- Podstawowy czytnik zbliżeniowy,
- Czytnik zbliżeniowy z klawiaturą,
- Programowalne wyjście.

Dodatkowe klawiatury strefowe powinny być dołączane do pętli dozorowej w ten sam sposób jak urządzenia detekcyjne, aby możliwie ograniczyć koszt i czas instalacji przewodów.

System powinien umożliwiać stosowanie kombinacji rozbrajania za pomocą klucza i hasła, albo oddzielnie.

Fizyczny klucz powinien być programowo przypisany do danego użytkownika. Rejestracja powinna się odbywać za pomocą oprogramowania służącego do konfiguracji centrali.

System powinien być w stanieysterować dowolne wyjście wirtualne i fizyczne w niemal nieograniczony sposób łącząc tryby logiczne AND, OR, opóźnienia aktywacji, priorytety i wyzwianie zdarzeń segregowanych według centrali, strefy, a także pojedynczego urządzenia. Relacje powinny być realizowane za pomocą standardowych funkcji a także rozszerzonych, które mogą wykorzystywać dodatkowo wejścia i wyjścia wirtualne, a także harmonogramy.

System powinien być w stanie oferować topologię pętli, dzięki której wszystkie czujniki będą się komunikowały ze sobą za pomocą dwóch żył. Rozwiązanie to zapewni ciągłe działanie systemu nawet w przypadku uszkodzenia pętli bądź uszkodzenia urządzenia.

Wszystkie urządzenia pętlowe oferowane przez dostawcę powinny posiadać wbudowane izolatory zwarć, co zapewni dodatkowe bezpieczeństwo dla ciągłej pracy systemu.

Elementy pętlowe powinny być w stanie przekazywać do centrali informacje na temat podstawowych alarmów takich jak wykrycie ruchu, antymasking, sabotaż, przy czym nie ma konieczności dokonywania dodatkowej parametryzacji czujników po podłączeniu do pętli.

Elementy pętlowe powinny być konfigurowalne z programu służącego do obsługi centrali bez konieczności dodatkowej fizycznej ingerencji w urządzenia.

Pojedyncza pętla dozorowa powinna oferować długość do 1000 m i możliwość podłączenia do 127 elementów detekcyjnych wykonanych w technologii pętlowej.

Pojedyncza centrala powinna być w stanie obsłużyć do ośmiu modułów pętlowych.

Moduły pętlowe powinny oferować dodatkowo dwa wyjścia zasilania dodatkowego w celu zapewnienia zasilania dla modułów służących do podłączenia czujników/urządzeń konwencjonalnych i zapewniania im lokalnie napięcia 12 V lub do innych zastosowań przewidzianych przez projekt.

System powinien umożliwiać tworzenie hybrydy wynikającej z połączenia technologii pętlowej i modułów urządzeń konwencjonalnych, dzięki czemu będzie możliwe stosowanie dedykowanych detektorów pętlowych, ale również pełnego portfolio detektorów konwencjonalnych.

Definiowanie urządzeń podłączonych bezpośrednio do pętli dozorowej powinno być możliwe za pomocą automatycznego wykrywania. Powinna istnieć możliwość przełączenia trybu pętli dozorowej w dwa odgałęzienia np. Dla celów serwisowych. W razie konieczności dodania urządzeń w sposób ręczny system powinien to umożliwiać poprzez czytelną funkcję „podnieś i upuść” realizowaną przez oprogramowanie konfiguracyjne.

### Panel główny centrali

Podstawowe funkcje:

- 1500 adresów
- 500 stref
- 996 użytkowników
- 8 nadzorowanych wejść i 1 nadzorowane wejście antysabotażowe
- 2 programowalne wyjścia przeznaczone np. dla optycznych i akustycznych urządzeń sygnalizacyjnych lub dla innych urządzeń powiadamiających.
- 2 programowalne wyjścia przekaźnikowe i 1 wyjście zasilania dodatkowego.
- 2 interfejsy magistrali do podłączenia do 32 klawiatur i 1 port Ethernet.
- możliwość zdalnej aktualizacji oprogramowania poprzez darmowe oprogramowanie komputerowe
- Raportowanie do stacji monitorującej powinno być możliwe przez: Ethernet, GPRS

Parametry elektryczne i środowiskowe:

<b>Zakres napięcia</b>	Od 19 VDC do 29 VDC, nominalnie 28 VDC
<b>Pobór prądu</b>	Od 250 mA do 500 mA
<b>Wyjścia</b>	1 wyjście zasilania dodatkowego i 2 wyjścia napięciowe
<b>Wyjścia przekaźnikowe</b>	2
<b>Pamięć</b>	Nieulotny nośnik pamięci dla konfiguracji i pamięci zdarzeń
<b>Temperatura pracy</b>	Od -10°C do 55°C
<b>Wilgotność względna</b>	Od 5% do 95%
<b>Wykorzystanie</b>	wewnętrzne

### Klawiatura

Podstawowe funkcje:

- Ekran dotykowy – 14 cm (5.7 cala) LCD z możliwością dostosowania jasności.
- Interfejs graficzny: 16-bitowy, Rozdzielczość 320 x 240
- Opcje językowe, definiowane dla użytkownika indywidualnie:
- DE, EN, FR, NL, HU, PL, RU, IT, ES, CZ, PT, LV.
- Jeżeli system nie jest gotowy do uzbrojenia, wówczas klawiatura powinna niezwłocznie pokazać rodzaj problemu. Dodatkowo powinna istnieć funkcja opcjonalnego wymuszonego uzbrojenia.
- Konfiguracja użytkownika: Dodawanie użytkownika, Usuwanie użytkownika, Edycja użytkownika, Zmiana hasła.
- Wbudowany przełącznik atysabotażowy.
- Struktura menu powinna być dostosowana do poziomu autoryzacji różnych użytkowników
- Poziom głośności i jasności powinny być indywidualnie dostosowywalne.
- Powinna istnieć możliwość aktualizacji oprogramowania wszystkich klawiatur w systemie jednorazowo za pośrednictwem darmowego oprogramowania komputerowego.

Parametry elektryczne i środowiskowe:

<b>Zakres napięcia</b>	Od 16 VDC do 29 VDC, nominalnie 28 VDC
<b>Pobór prądu</b>	Uruchamianie: 800mA Alarm: 175mA Ekran bezczynny 100mA Ekran bezczynny wygaszony: 60mA Od 250 mA do 500 mA
<b>Ekran</b>	
Typ	TFT-LCD
Przekątna w cm	14
Proporcje obrazu	4:3
Rozdzielczość w pikselach	320 x 240
Głębina kolorów	16-bit
<b>Temperatura pracy</b>	Od -10°C do 55°C
<b>Wilgotność</b>	Od 5% do 95%
<b>Klasy bezpieczeństwa</b>	IP31 IK06

### Czujka PIR Grade 3

Czujki z antymaskingiem i interfejsem magistrali są przeznaczone do wewnętrznych zastosowań komercyjnych i o podwyższonych wymaganiach ochrony. Czujka pracuje w sieci wysyłając sygnały alarmu, usterki, sabotażu oraz antymaskingu poprzez szeregowo połączone komunikacyjne magistrali. Technologia MANTIS(Multi-point Anti-mask with Integrated Spray detection, wielopunktowy antymasking ze zintegrowanym wykrywaniem zamalowania soczewki sprayem) wykorzystano opatentowane soczewki pryzmatyczne i system aktywnego wykrywania promieniowania podczerwonego, zapewniające najlepszą w branży ochronę przed wszystkimi znanymi formami ataku. Technologia MANTIS spełnia najnowsze międzynarodowe normy dotyczące wykrywania obiektów zakrywających lub zasłaniających pole widzenia czujki. Czujka została wyposażona w wbudowany czujnik poziomu światła, który aktywnie redukuje światło białe w celu wyeliminowania fałszywych alarmów wywoływanych przez źródła jasnego światła.

**Czujka posiada Certyfikat EN50131-2-4 Grade 3** pozwalający na instalację elementu w instalacjach o średnim lub wysokim stopniu ryzyka.

**Podstawowe funkcje:**

- Standardowy zasięg 12x12 m, możliwość wyboru krótkiego zasięgu 8 x 10 m
- TriTech. Technologia pasywnej podczerwieni oraz mikrofalowy radar Dopplerowski z technologią FSP(First Step Processing) zapewniają doskonałą skuteczność wykrywania i najlepszą w swojej klasie odporność na fałszywe alarmy
- Adaptacyjne przetwarzanie mikrofalowe zakłóceń –zmniejszona liczba alarmów wywoływanych powtarzającymi się sygnałami
- Technologia wielopunktowego antymaskingu ze zintegrowanym wykrywaniem zablokowania soczewki sprayem — wykrywa próby ograniczenia pole widzenia czujki
- Technologia wykrywania maskowania i kamuflażu (C2DT) maksymalizuje skuteczność wykrywania intruzów, którzy próbują zamaskować swój sygnał podczerwieni.

<b>Zakres napięcia LSN</b>	9-29 VDC
<b>Pobór prądu LSN</b>	5 mA( wskaźnik zasilania MAP 27)
<b>Wilgotność względna pracy</b>	0-95% bez kondensacji
<b>Temperatura pracy</b>	-10°C ÷ +55°C
<b>Stopień ochrony</b>	IK04(EN 50102)
<b>Wyjścia</b>	Komunikacja szeregową przez magistralę LSN

### Adresowalny KONTAKTRON

Styk magnetyczny do montażu powierzchniowego jest używany do monitorowania otwarcia drzwi i okien. Styk ma nadzór antysabotażowy, gdy magnes zewnętrzny zostanie zwarty, styk antysabotażowy jest aktywowany i wysyłany jest raport.

#### Podstawowe funkcje:

- Styk magnetyczny do montażu powierzchniowego do monitorowania otwarcia drzwi i okien
- Nadzór antysabotażowy
- Montaż równoległy
- Instalacja na materiałach ferromagnetycznych jest dopuszczalna w obudowie EG2 do montażu płaskiego
- Do podłączenia do systemów bezpieczeństwa

### Detektor zbitcia szyby Grade 3

Detektor daje informacje w postaci alarmu, gdy dokonana jest próba włamania poprzez zbitcie szyby w oknie, oszklonych drzwiach lub innych szklanych elementach w ścianie. Detektor jest przeznaczony do stosowania wewnątrz pomieszczeń. Zakres działania wynosi od 1 do 9 m. Kąt pokrycia wynosi 165°, co oznacza, że jeden detektor może chronić kilka okien w jednym pomieszczeniu. Detektor może być zamontowany zarówno na suficie, jak i na ścianie. Detektor jest wyposażony w funkcję aktywnego antymaskingu, której głównym celem jest wykrywanie prób uszkodzenia lub zaślepienia mikrofonu. Detektor został wykonany w zgodności z normą PN-EN 50131-2-7-1:2013-06/A1, stopień zabezpieczenia 3.

Typ (grubość) chronionego szkła	Zwykłe (4 mm), laminowane P2,P4( 4 mm + 4 mm)
Rozmiar chronionej szyby	Min 40x40 cm
Napięcie zasilania	8 – 30 V, DC
Pobór prądu w stanie czuwania	12 mA przy 12 V,

	7.3 mA przy 24 V
<b>Zakres temperatur pracy</b>	+5°C do +40°C
<b>Wilgotność środowiska pracy</b>	Max. 93% RH

### Zewnętrzny sygnalizator akustyczno-optyczny Grade 3

Sygnalizator optyczno-akustyczny z wbudowanym akumulatorem NiMH 7.2 V 330 mAh. Sygnalizator posiada szereg zabezpieczeń: przed otwarciem obudowy, oderwaniem od ściany, próbą sabotażu poprzez zapiankowanie. Sygnalizator posiada certyfikat **EN50131-1:2006+A1:2009 Grade 3** pozwalający na instalację elementu w instalacjach o średnim lub wysokim stopniu ryzyka.

#### Podstawowe funkcje:

- Obudowa o bardzo niskim profilu
- Diagnostyka dzięki zastosowanej diodzie LED
- Tryb oszczędzania lampy stroboskopowej po godzinie pracy
- Możliwość wyboru dwóch typu alarmu(SAB/SCB)
- Wyjście awarii systemu

<b>Wyjście akustyczne</b>	115 dB(A) -w odległości 1 m
<b>Typ lampy</b>	Xenon
<b>Akumulator</b>	Ni-MH 7,2 330 mAh
<b>Pobór prądu w trybie alarmu</b>	360 mA
<b>Pobór prądu w stanie spoczynku</b>	40 mA

### Wewnętrzny sygnalizator akustyczno-optyczny GRADE 3

Sygnalizator wewnętrzny akustyczno-optyczny. Opracowany z myślą o obiektach średniego oraz wysokiego ryzyka. Posiada pełną zgodność z EN50131 dla stopnia GRADE 3. Zabezpieczenie antysabotażowe sygnalizatora jest realizowane zarówno dla zdjęcia pokrywy jak i oderwania od podłoża.

#### Podstawowe funkcje:

- Obudowa o bardzo niskim profilu
- Niski pobór prądu
- Możliwość instalacji w systemach bezpieczeństwa wymagających zabezpieczenia w stopniu GRADE 3
- Zabezpieczenie antysabotażowe:
  - przed otwarciem
  - przed oderwaniem od podłoża

<b>Napięcie zasilania</b>	12 VDC
<b>Zakres napięć zasilania</b>	9-15 VDC
<b>Natężenie dźwięku</b>	112 dB- w odległości 1 m
<b>Pobór prądu w trybie sygnalizacji optycznej</b>	17 mA przy 12 VDC
<b>Pobór prądu w trybie sygnalizacji optycznej + akustycznej</b>	100 mA przy 12 VDC
<b>Temperatura pracy</b>	-15°C do +40°C

### Montaż urządzeń

Dokładne rozmieszczenie urządzeń zostało pokazane na planie instalacji SSWiN.

Wszystkie elementy instalacji powinny być oznaczone alfanumerycznie, w sposób trwały. Nie dopuszcza się oznaczeń w postaci pisania na powłokach kablowych, należy stosować specjalne trwałe oznaczniki. Te same oznaczenia powinny być użyte w urządzeniach monitorujących, sterujących, wizualizujących system oraz w dokumentacji powykonawczej. Przewody należy instalować tak, aby chronić je przed uszkodzeniami w rurkach ochronnych możliwie z dala od instalacji mogących mieć wpływ na funkcjonowanie systemu. Przejścia przewodów instalacji przez ściany zewnętrzne oraz wewnętrzne pomiędzy strefami pożarowymi uszczelnić przy pomocy mas uszczelniających o odporności właściwej dla ścian, które są uszczelniane.

Montaż wszystkich urządzeń wykonać zgodnie z DTR poszczególnych urządzeń oraz według wytycznych producenta.

### **Zalecenia uruchamiania, eksploatacji i konserwacji**

Przed przekazaniem systemu do eksploatacji zaleca się dokładne sprawdzenie systemu i przeprowadzenie prób funkcjonalnych oraz przeprowadzenie pomiarów sprawdzających wszystkich łączy. Należy również wykonać dokumentację powykonawczą oraz przeszkolić pracowników obsługujących system.

### **Wyliczenia akumulatorów do centrali SSWiN**

Desired Performance (user input)		
Desired Standby time (hours)	60	
Desired Alarm time (minutes)	15	
Desired Derating Factor (percentage)	10%	
Calculated values	Standby Power (Watt)	Alarm Power (Watt)
Main panel component	2,14	2,14
DE Module component	0,00	0,00
Power supply components	6,72	6,72
Control Center components	8,40	14,88
CAN splitter components	0,00	0,00
User Defined Additional Devices	0,00	0,00
LSN Gateway components	9,14	9,42
GLT(AUX) components	0,00	0,00
Subtotal	26,40	33,16
Power requirements	Power (Watt - hour)	
Standby time power required	1577,7	
Alarm time power required	8,3	
Power Requirements subtotal = Standby + Alarm	1586,0	
Power requirements derating	158,6	
Power Requirements total = Subtotal + Derating	1744,5	
TOTAL BATTERY DEMAND in Ampere-hour [Ah]	73	

**Zestawienie podstawowych materiałów:**

Lp.	Opis	Ilość
1.	Zestaw centrali SSWiN (1 panel, 1 zasilacz, 1 brama, 1 klawiatura główna, 1 obudowa, 1 moduł)	1
2.	Zasilacz do kontrolera (do 32 na system)	1
3.	Obudowa zasilania dodatkowego (zestaw z blokiem zacisków AC, tamperem i zamkiem). Może pomieścić 1xZasilacz, 4xakumulator 40Ah	1
4.	Akumulator 12V/40Ah	4
5.	Panel sterowania P, manipulator, kolorowy ekran dotykowy (do 32 na system)	2
6.	Czujka dualna PIR+MW , Antymasking wielopunktowy, 12m x 12m	28
7.	Czujka magnetyczna, montaż powierzchniowy, Tamper, (VdS C)	40
8.	Moduł do linii konwencjonalnych 6 wejść i 4 wyjścia	3
9.	Moduł przekaźnikowy dla EMIL, 2 przekaźniki	4
10.	Tamper dla EMIL	3
11.	Konwencjonalny przycisk napadowy Grade 3	1
12.	Konwencjonalna czujka zbita szyby Grade 3	4
13.	Sygnalizator optyczno akustyczny Grade 3: wew	4
14.	Sygnalizator optyczno akustyczny Grade 3: zew	1
15.	Zasilacz 13,8V/10A/65Ah/EN zasilacz buforowy impulsowy Grade 3	1
16.	Akumulator 12V/65Ah	1

**20. INSTALACJA MULTIMEDIALNA**

W budynku projektuje się instalacje multimedialną.

Materiał wideo przekazywany jest z poziomu małych komputerów (NUC) umieszczonych w pobliżu projektorów i monitorów interaktywnych (lub po prostu na nich) – połączenie za pomocą krótkich kabli HDMI.

Całością steruje urządzenie – jednostka sterująca główna.

W sali -1.6 należy wykonać okablowania między projektorem a miejscem podłączenia komputera dla prelegenta (lokalizację tego miejsca ustalić na budowie) .

Dodatkowo dla nagłośnienia przewiduje się podłączenia do każdego projektora niezależnych dwóch głośników, poprzez wzmacniacz.

Instalację wykonać zgodnie z opisem funkcjonowania oraz schematem ideowy i instrukcją producenta wybranych urządzeń .

**UWAGA**

- Funkcjonalność systemu potwierdzić z Użytkownikiem na etapie wykonawstwa
- Wykonanie systemu powinna wykonać firma posiadająca doświadczenie w tego typu instalacjach.
- Przed ułożeniem przewodów potwierdzić typ okablowania u wybranych dostawców urządzeń.

**Specyfikacja podstawowych urządzeń systemu :**

<b>EKRAN DOTYKOWY Z GŁOŚNIKAMI</b>	
<b>Wygląd</b>	cienkie ramki
<b>Przekątna</b>	65"
<b>Touch Glass</b>	Powłoka antypośliskowa, szkło antyodblaskowe, matowa, polerowana powierzchnia, bardzo płynne pisanie,
<b>Rozdzielczość fizyczna</b>	3840 x 2160 (4K UHD)
<b>Format obrazu</b>	16:9

<b>Jasność min.</b>	400 cd/m <sup>2</sup>
<b>Przepuszczalność światła min.</b>	90%
<b>Kontrast statyczny</b>	4000:1
<b>Dynamic contrast</b>	5000:1
<b>Czas reakcji (GTG) max.</b>	10ms
<b>Kąty widzenia</b>	poziomo/pionowo: 178°/178°
<b>Synchronizacja pozioma</b>	30 - 150kHz
<b>Plamka</b>	0.372mm
<b>Obudowa</b>	czarna, matowa
<b>Technologia dotykowa</b>	Tak
<b>Punkty dotykowe</b>	50
<b>Dokładność dotyku</b>	+/- 2mm
<b>Interfejs dotykowy</b>	TAK
<b>Dotyk wykonywany</b>	stylusem, palcem, w rękawiczce
<b>Obsługiwane systemy operacyjne</b>	kompatybilne z systemami Windows i Linux
<b>Cyfrowe wejścia sygnału min.</b>	HDMI x2 (2.0, max. 3840x2160 DisplayPort x2 (1.4, max. 3840x2160)
<b>Wejścia audio</b>	Mini jack
<b>Cyfrowe wyjścia sygnału</b>	HDMI x1 (2.0, max. 3840x2160) USB-C x1 (3.1, 3840x2160 )
<b>Port USB</b>	odtwarzanie multimediiów / urządzenia peryferyjne / pamięć masowa
<b>RJ45 (LAN)</b>	Tak,
<b>Mikrofon</b>	Wykrywanie głosu min.6 m
<b>Wbudowane głośniki min.</b>	Wbudowane głośniki 2 x 8W
<b>Zintegrowane oprogramowanie</b>	Android 13 OS lub nowszy, przeglądarkę sieci WWW, system zarządzania plikami,
<b>WiFi</b>	tak (Moduł WiFi 6 - Dwuzakresowy moduł WiFi (2,4 GHz / 5 GHz), Standard Wi-Fi: IEEE 802.11 a / b / g / n / ac, Obsługa Bluetooth: 2.1 / 3.0 / 4.2 / 5.0)
<b>Hardware min.</b>	CPU: Quad core, RAM: 8GB, ROM: 64GB
<b>Tryb kiosk</b>	24/7
<b>Twardość szkła</b>	7h
<b>Języki menu OSD</b>	PL
<b>Parametry regulowane</b>	ustawienia ogólne (wejście, głośność, podświetlenie), ustawienia dźwięku (głośność, wysokie tony, balans, tryb dźwięku, wycisz), ustawienia wyświetlacza (jasność, kontrast, odcień, ostrość, tryb wyświetlania,), ustawienia (sieć bezp)
<b>Akcesoria</b>	Zamawiający wymaga dostarczenia uchwytu montażowego wraz z wyrzyskimi wymaganymi kablami do podłączenia.
<b>Pilot</b>	Tak
<b>Zasilacz</b>	wewnętrzny
<b>Zasilanie</b>	AC 100 - 240V, 50/60Hz
<b>Zużycie energii max.</b>	240 W typowo, 1 W stand by, 0.5W off mode
<b>Certyfikaty</b>	CE, TUV-Bauart, EAC, RoHS support, ErP, WEEE, REACH (RoHS)
<b>Gwarancja</b>	5 lata

<b>PROJEKTOR</b>	
<b>Technologia</b>	3LCD (3x0,76")
<b>Źródło światła</b>	Dioda Laserowa (Grupa Ryzyka 2)
<b>Rozdzielczość natywna</b>	1920 x 1200 pikseli
<b>Maksymalna obsługiwana rozdzielczość</b>	4096 x 2160 pikseli
<b>Jasność</b>	8 000 ANSI lumenów
<b>Kontrast dynamiczny</b>	3 000 000:1 (zgodność z ISO21118-2012 lub nowszą)
<b>Kolory</b>	10 bit
<b>Dołączony obiektyw</b>	Współczynnik projekcji: 0.79 - 1.11 :1
<b>Ogniskowa</b>	13.3 - 18.6 mm
<b>Przysłona</b>	2.0 - 2.5
<b>Optymalny dystans projekcji</b>	0.8 - 12m
<b>Elektryczny zoom i focus</b>	TAK
<b>Elektryczne przesuwanie obiektywu</b>	Pionowo +10% / -50% Poziomo +/- 20%
<b>Automatyczna korekcja zniekształceń trapezowych</b>	Pionowo i poziomo +/- 40°
<b>Wejścia wideo</b>	1x D-SUB (component) 1x Display Port (HDCP) 2x HDMI (HDCP 2.2) 1x HDBaseT (HDCP 2.2)
<b>Wyjścia wideo</b>	1x HDBaseT
<b>Wejścia / wyjścia audio</b>	x6 / x1
<b>Złącze do synchronizacji 3D</b>	x1 (złącze 3-pinowe)
<b>Funkcja PiP</b>	TAK (obraz w obrazie) (obraz obok obrazu)
<b>Poziom szumu max.</b>	30dB
<b>Funkcjonalność</b>	<p>Całkowicie szczelny laserowy silnik optyczny, w połączeniu z technologią LCD, konstrukcja całkowicie bezfiltrowa</p> <p>Możliwość pracy w orientacji pionowej oraz swobodnie wychylanie projektora</p> <p>Pamięć ustawień obiektywu: minimum 2 presety</p> <p>Tryb zapewniający jednakową jasność obrazu, przez cały okres użytkowania</p> <p>Zarządzanie za pomocą oprogramowania dostarczanego przez producenta projektora, oraz za pomocą przeglądarki www</p> <p>Wsparcie dla funkcji łączenia krawędzi i funkcji stacking</p> <p>Zgodność ze standardem zapewniającym szeroki zakres dynamiki tonalnej</p> <p>Wyświetlanie przestrzeni kolorów REC2020, REC709, REC601</p> <p>Regulacja poziomu kolorów RGBCMY, dostosowywanie barwy i nasycenia</p> <p>Niezależna regulacja ostrości w centrum obrazu i na obrzeżach</p> <p>Tryb kompensacji kolorów przy konfiguracji wieloekranowej</p>
<b>Akcesoria</b>	Zamawiający wymaga dostarczenia uchwytu montażowego wraz z wyrzyskimi wymaganymi kablami do podłączenia.
<b>Gwarancja</b>	3 lata lub 10,000 godzin na lampę (w zależności od tego, co nastąpi wcześniej)

## EKRAN PROJEKCYJNY

Format:

Wymiar pow. aktywnej (wersja bez obramowania) [cm/cale]:

Wymiar pow. aktywnej (wersja z obramowaniem) [cm/cale]:

Wymiary kasety (dł. x wys. x gł.) [cm]:

Wysuw pow. projekcyjnej:

Strona wyprowadzenia przewodu zasilania:

1 : 1

300 x 300 / 167"

290 x 290 / 161"

307.0 x 15.0 x 13.0

tylni (domyślnie) / przedni

prawa (domyślnie) / lewa

### GŁOŚNIK ŚCIENNY

- **Pasmo przenoszenia (-10 dB):** 90Hz – 20kHz
- **Nominalna wysoka impedancja:** Linia 100 V
- **Nominalna niska impedancja:** 8Ω
- **Selektor mocy @ 100V:** 5, 7,5, 15, 30 W
- **Moc skuteczna:** 50W
- **Czułość (dB@1m 1W):** 92,5 dB

## WZMACNIACZ

### Kluczowe cechy

- Wzmacniacz 2 x 20 WRMS @ 4Ω z trybami wyjścia STEREO, PARALLEL i BRIDGE
- 1 wejście symetryczne MIC, z zasilaniem Phantom i wysokiej klasy przedwzmacniaczem, w tym bramka szumów i funkcja talkover na pozostałych wejściach
- 2 niebalansowane wejścia LINE
- 2-zakresowa regulacja tonów (Bass, Treble) niezależna, dla szyn MIC i LINE
- Wyjście AUX do podłączenia zewnętrznego do innych urządzeń lub wzmacniaczy
- Cyfrowe sterowanie lokalne, typ enkodera
- Pilot na podczerwień w zestawie
- Pilot kompatybilny z WPmVOL i WPmVOL- Panele ściennie SR (0-10 VDC)
- Port sterowania RS-232 kompatybilny z oprogramowaniem EclerCOMM i protokołem CA-NET
- Port MUTE do zewnętrznego wyciszania urządzenia w przypadku konieczności uruchomienia systemu ewakuacji
- Zarządzanie ustawieniami/źródłami przez port zdalnego sterowania RS-232 lub 0-10 VDC
- Funkcja AUTO STANDBY
- Lekka i cicha konstrukcja (bez wentylatora)
- **Stereofoniczny 4Ω:** 22 WRMS
- **Zmostkowane 8Ω:** 36 WRMS
- **8Ω stereo:** 10 WRMS
- **Pilot:** Pilot na podczerwień w zestawie + 1 porty REMOTE (regulacja wyboru i głośności) + RS232 (kompatybilny z protokołem EclerCOMM i CA-NET)
- **Wymiary:** 155x155x45mm

## KOMPUTER

Rodzaj produktu

Mini-PC

Przekątna wyświetlacza (cm)

2.5 cm

Przekątna wyświetlacza

1.0 cal

Seria procesora

Intel® Core™ i5	
<b>Procesor</b>	Intel® Core™ i5 i5-12400T 6x 1,8 GHz
<b>Procesor / Model</b>	i5-12400T
<b>Generacja procesora</b>	12. Gen. (Jezioro Olchowe)
<b>Ilość rdzeni procesora</b>	6 x
<b>Częstotliwość taktowania procesora</b>	1.8 GHz
<b>Częstotliwość taktowania turbo (max.)</b>	4.2 GHz
<b>Rdzenie wydajności procesora (liczba)</b>	0
<b>Rdzenie wydajności procesora (liczba)</b>	6
<b>Wydajność procesora Rdzenie Boost Clock</b>	1.8 GHz
<b>Wydajność procesora Rdzenie Boost Clock</b>	4.2 GHz
<b>Procesor / Cache</b>	18 MB
<b>Pamięć RAM</b>	8 GB
<b>Typ pamięci</b>	DDR4-SDRAM
<b>Taktowanie pamięci</b>	3200 MHz
<b>Ilość slotów pamięci</b>	1
<b>RAM / max. wyposażenie</b>	64 GB
<b>Wbudowana karta graficzna</b>	Tak
<b>Wbudowany adapter graficzny (producent GPU)</b>	Intel
<b>Oddzielna karta graficzna</b>	Nie
<b>Pojemność dysku SSD (całkowita)</b>	256 GB
<b>SSD 1 Typ</b>	SSD
<b>Pojemność SSD 1</b>	256 GB
<b>Złącze SSD 1</b>	M.2 PCIe NVMe
<b>Wbudowany napęd</b>	Bez napędu
<b>Wersja Bluetooth®</b>	5.2
<b>Mobilny Internet (LOV)</b>	WiFi
<b>Interfejsy: DisplayPort</b>	1 x
<b>Interfejsy: Gigabit-LAN</b>	1 x
<b>Interfejsy: HDMI</b>	1 x
<b>Interfejsy: USB 2.0 (płyta główna)</b>	1 x
<b>Ilość USB 3.1 Gen 1</b>	1 x
<b>Ilość USB 3.1 Gen 2</b>	4 x
<b>Ilość USB-C™</b>	1 x
<b>Interfejsy (komputerowe/multimedialne)</b>	USB 3.2 Gen 1 (USB 3.0)

USB-C®  
HDMI  
mikrofon / słuchawki (jack 3,5 mm)  
LAN (10/100/1000 MBit/s)  
USB 3.2 Gen 2 (USB 3.1)  
DisplayPort  
USB 2.0

**Kolor**

czarny

**Szerokość produktu**

179 mm

**Wysokość produktu**

36.5 mm

**Głębokość produktu**

182.9 mm

**Waga**

1.25 kg

**System operacyjny**

FreeDOS

## JEDNOSTKA STERUJĄCA

Jednostka sterująca to wysokowydajny, kompaktowy procesor sterujący przeznaczony do scentralizowanego sterowania AV w małych i średnich aplikacjach. Jednostka sterująca obsługuje również zaawansowane standardy bezpieczeństwa i Gigabit Ethernet, co zapewnia kompatybilność z wieloma panelami dotykowymi TouchLink® Pro, panelami przycisków sieciowych i interfejsami rozszerzeń przy użyciu standardowej infrastruktury sieciowej. Jednostka sterująca to idealny wybór do zastosowań AV, które wymagają wydajnego, a jednocześnie kompaktowego procesora sterującego.

### Cechy

- **Obsługuje panele dotykowe, panele przycisków sieciowych i interfejsy rozszerzeń**
- **Obsługuje bezpieczne protokoły komunikacyjne będące standardami branżowymi** — korzysta ze standardowych protokołów komunikacyjnych, w tym HTTP (niezabezpieczone), HTTPS, SSH, SFTP, SMTP, NTP, Discovery Service, DHCP, DNS, ICMP, 802.1X i IPv4.
- **Monitorowanie i kontrola Ethernet** — zarządzaj, monitoruj i kontroluj urządzenia AV za pomocą standardowej sieci Ethernet.
- **Jeden dwukierunkowy port szeregowy RS-232/RS-422/RS-485 z uzgadnianiem sprzętowym i programowym**
- **Obsługuje 10/100/1000Base-T**
- **Obsługuje popularne protokoły BMS – Building Management System, takie jak BACnet, KNX i DALI** . Protokoły te umożliwiają scentralizowane monitorowanie i sterowanie systemami mechanicznymi i elektrycznymi, w tym HVAC, oświetleniem, zasilaniem, przeciwpożarowym i bezpieczeństwem.
- **Centralne wdrożenie — Użyj głównego procesora sterującego do wdrożenia wszystkich plików systemowych, konfiguracji i programów** — Szybkie wdrożenie systemu sterowania poprzez przesłanie wszystkich plików projektu do głównego procesora sterującego. Główny procesor sterujący automatycznie prześle pliki do innych paneli dotykowych, procesorów sterujących i paneli przycisków w tym systemie, gdy tylko zostaną one przełączone w tryb online.
- **Obsługuje urządzenia sterowane przez Ethernet** — umożliwia sterowanie wieloma urządzeniami AV obsługującymi Ethernet, takimi jak wyświetlacze, przełączniki i źródła.
- **Automatyczna synchronizacja zegara umożliwia panelowi dotykowemu wyświetlanie dokładnej godziny i daty**
- **Obsługuje synchronizację systemu sterowania** — synchronizacja umożliwi użytkownikom zachowanie i przywrócenie stanu skonfigurowanych punktów końcowych w przypadku awarii sieci lub zasilania.
- **Wskaźniki stanu portów na panelu przednim**

- **Wielopoziomowa ochrona hasłem** — umożliwia ustawienie zabezpieczeń w oparciu o role użytkowników.
- **Obsługuje uwierzytelnianie 802.1X** — zapewnia obsługę standardu uwierzytelniania IEEE 802.1X dla kontroli dostępu do sieci opartej na portach.
- **Kompaktowa obudowa metalowa o wysokości 1U i szerokości ćwierć stojaka**

#### Zestawienie podstawowych urządzeń

Lp.	Opis	Ilość
<b>Sala edukacyjno-historyczna (-1.6)</b>		
1	Projektor	1
2	Obiektyw	1
3	Ekran projekcyjny 300cm	1
4	Trigger	1
5	Transmisja HDMI	1
6	Głośnik ścienny	2
7	Wzmacniacz	1
8	Przyłącze stołowe/ ścienne (opcja)	1
9	Monitor interaktywny	1
10	Uchwyt ścienny monitora	1
11	Komputer	1
12	Panel sterujący(opcja)	1
13	Podstawka do panela(opcja)	1
14	Access Point	1
<b>Hol z szafkami (-1.7)</b>		
1	Monitor interaktywny	1
2	Uchwyt ścienny monitora	1
3	Komputer	1
<b>Sala ekspozycji (0.4)</b>		
1	Projektor	1
2	Obiektyw	1
3	Ekran projekcyjny 300cm	1
4	Trigger	1
5	Głośnik ścienny	2
6	Wzmacniacz	1
7	Komputer	1
<b>Hol wejściowy (0.5)</b>		
1	Monitor interaktywny	1
2	Uchwyt ścienny monitora	1
3	Komputer	1
<b>System sterowania (serwerownia)</b>		
1	Jednostka sterująca	1
2	Switch LAN	1
3	Router	1
4	Access Point	1
5	Panel sterujący	1
6	Podstawka do panela	1

Prace instalacyjne		
1	Okablowanie	1 - kpl
2	Programowanie	1
3	Montaż, uruchomienie	1- kpl

### Wytyczne instalacyjne

Trasy sygnałowe audio należy prowadzić wydzielonymi trasami. Dopuszcza się prowadzenie tras głośnikowych w korytach razem z innymi instalacjami niskoprądowymi, jednak koryta te muszą być wydzielone od tras elektrycznych.

## 21. SYSTEM DETEKCJI WYCIEKU

Opracowanie dotyczy projektu zabezpieczenia oraz monitoringu pomieszczeń Muzeum im. Jacka Malczewskiego w Radomiu w zakresie detekcji wycieków. Zastosowane rozwiązanie będą tworzyć przewody i taśmy sensoryczne oraz czujniki punktowe.

System detekcji wycieków jest układem scentralizowanym i opiera się na jednej autonomicznej centrali zbierającej sygnały od wszystkich czujników. Centrala informuje użytkownika o wycieku/awarii/braku zasilania poprzez sygnały optyczno-akustyczne generuje historię zdarzeń, ma możliwość regulacji czułości. Projektuje się centralę 24 strefową z wykorzystaniem 24 stref umieszczoną w pomieszczeniu ochrony 0.7 na parterze.

Rodzaj czujników oraz proponowane rozwiązania zostały dobrane w sposób zapewniający skuteczną detekcję dla każdego rodzaju pomieszczenia.

- Pomieszczenia magazynów oraz sale wystawowe zostaną zabezpieczone poprzez montaż taśmy sensorycznej obwodowo w pomieszczeniu.
- Pomieszczenie serwerowni zostanie zabezpieczone poprzez zastosowanie przewodu sensorycznego M8 poprowadzonego po obwodzie pomieszczenia. Przewody sensoryczne oraz taśma mocowane są do podłoża za pomocą klipsów samoprzylepnych i ułożone równo wzdłuż ścian.
- Pomieszczenie węzła c.o., wentylatornia oraz pomieszczenie wodomierza zostanie zabezpieczone poprzez montaż czujników punktowych. Umieszcza się je na ścianie, przy drzwiach w niewielkiej odległości od posadzki, tak aby sondy czujnika mogły wykryć wyciek.

Wszystkie stosowane czujniki natychmiastowo odbiorą sygnał o wycieku i przekażą go do centrali systemu. Ta wygeneruje alarm, który powiadomi użytkownika poprzez sygnały optyczno-akustyczne. Dodatkowo przewiduje się podłączenie systemu detekcji wycieków z systemem nadrzędnym BMS. Użytkownik otrzyma wtedy natychmiastową informację oraz pełną kontrolę nad wyciekiem. System nadrzędny wygeneruje komplet zdarzeń i obraz, który da użytkownikowi możliwość sprawdzenia dokładnej lokalizacji źródła wycieku oraz numeru i nazwy pomieszczenia. Do systemu nadrzędnego centrala wyprowadza informację o:

- wycieku na każdej ze stref i linii,
- uszkodzeniu na każdej ze stref i linii,
- rezystancja każdej ze stref,

- wyciek na metrze,
- rejestr zdarzeń,
- brak zasilania,
- rejestr uszkodzeń.

Zestawienie pomieszczeń i rodzaj zabezpieczenia:

	Numer pomieszczenia	Nazwa pomieszczenia	SYSTEM ILOŚĆ STREF	ZABEZPIECZENIE
POZIOM -1	-1.3	Węzeł C.O.	2	Czujnik punktowy
	-1.4	Pomieszczenie wodomierza	1	Czujnik punktowy
	SUMA		3	
PARTER	0.3	Sala ekspozycji	2	Taśma sensoryczna
	0.4	Sala ekspozycji	2	Taśma sensoryczna
	0.5	Sala ekspozycji	2	Taśma sensoryczna
	0.8	Sanitariat damski oraz dla niepełnosprawnych	1	Czujnik punktowy
	0.9	Sanitariat męski	1	Czujnik punktowy
	0.11	Gabinet Ignacego Zabiełły	1	Taśma sensoryczna
POZIOM +1	SUMA		9	
	1.2	Magazyn	1	Taśma sensoryczna
	1.4	Magazyn	1	Taśma sensoryczna
	1.5	Magazyn	1	Taśma sensoryczna
	1.9	Sanitariat personelu	1	Czujnik punktowy
	1.10	Pomieszczenie socjalne	1	Taśma sensoryczna
	1.13	Wentylatornia	2	Czujnik punktowy
	1.14	Serwerownia	4	Przewód sensoryczny
	1.15	Magazyn	1	Taśma sensoryczna
SUMA			13	
CAŁKOWITA ILOŚĆ STREF			24	

Wymagania jakie powinienem spełniać system:

#### SPECYFIKACJA CENTRALI:

- System jest dedykowany tylko do detekcji wycieków cieczy.
- Centrala posiada możliwość **indywidualnej** regulacji czułości wykrywania wycieku dla każdej ze stref osobno (zakres regulacji od 25 kOhm do 500 kOhm).
- System rozróżnia sygnał wycieku od sygnału uszkodzenia czujnika lub uszkodzenia układu.
- System jest hybrydowy, tj. ma możliwość podłączenia stref oraz linii wykrywających wyciek na danym metrze bezpośrednio do panelu bez stosowania urządzeń zewnętrznych.
- System ma możliwość komunikacji po protokole Modbus TCP/IP.
- Sygnał wycieku precyzyjnie wskazuje miejsce (lub pomieszczenie) w którym doszło do wycieku/awarii dla obszaru danej strefy.
- System jest samotestujący, tzn. sprawdza poprawność działania podłączonych czujników, sygnalizując zmianę stanu w czasie rzeczywistym.
- Strefy kontroli są odseparowane (zdarzenie w jednej strefie nie ma wpływu na ciągłość monitorowania pozostałych stref).
- System posiada historię minimum 1000 ostatnich zdarzeń.
- System posiada przemysłowy panel kontrolny wyświetlający wszystkie zdarzenia oraz sterowalny za pomocą strzałek i klawiszy.

- System ma możliwość dodania użytkowników, nadania im odpowiednich uprawnień (użytkownik / administrator). Ponadto każdy użytkownik powinien mieć swoje indywidualne hasło w celu rozróżnienia w historii osoby resetującej / konfigurujecej system.
- System ma możliwość wczytania parametrów oraz wgrania aktualizacji oprogramowania za pomocą USB.
- System ma możliwość zmiany języka obsługi (polski / angielski).
- System ma możliwość przywrócenia ustawień fabrycznych.
- System ma możliwość podglądu aktualnej rezystancji na wszystkich strefach z poziomu panelu operatorskiego.
- System ma możliwość konfiguracji wejść centrali – analogowe lub cyfrowe.
- System ma możliwość modułowej rozbudowy o kolejne strefy (dołożenie karty dodatkowych wejść).
- System ma możliwość sterowania innymi urządzeniami automatyki budynków (zawory, pompy, inne).
- System posiada zasilanie awaryjne oraz optycznie sygnalizuje niski poziom zasilania awaryjnego.
- System posiada optyczną sygnalizację braku zasilania.
- System posiada komplet indywidualnych, **programowalnych (NO lub NC) oraz dowolnie konfigurowalnych** przekaźników do każdej ze stref, które zmieniają stan podczas występowania alarmów. Konfiguracja powinna dotyczyć możliwości przydzielenia do każdego przekaźnika różnej konfiguracji alarmów.
- System posiada cztery **programowalne** oraz **dowolnie konfigurowalne** przekaźniki bezpotencjałowe (NO/COM/NC) które zmieniają stan podczas występowania alarmów. Konfiguracja powinna dotyczyć możliwości przydzielenia do każdego przekaźnika różnej konfiguracji alarmów.
- System ma możliwość współpracy z systemami nadrzędnymi np. BMS poprzez wyjścia przekaźników lub magistralę RS 485 (np. Protokół ModBUS).
- System jest niezależny od warunków otoczenia (temperatury, wilgotności).
- System powinien mieć możliwość rozbudowy o czujniki mające możliwość wykrywania wycieków cieczy przewodzących oraz nieprzewodzących prądu.
- System powinien mieć możliwość rozbudowy o przewody sensoryczne niechłonna wilgoci z powłoką syntetyczną.
- Stosowane taśmy sensoryczne (chłonna wilgoć) powinny być zabezpieczone przed korozją oraz wykonane z linki.
- Stosowane czujniki punktowe powinny być zabezpieczone przed możliwością uszkodzenia za pomocą obudowy ze stali nierdzewnej.
- Instalacja powinna zawierać detektory liniowe i punktowe.
- System powinien mieć możliwość zastosowania różnego rodzaju urządzeń detekcyjnych np. czujników oleju, czujników dywanowych, czujników punktowych w pozycji pionowej i poziomej, taśm wykrywających, minimum 5-cio strefowych czujników liniowych.

## **22. SYSTEM PRZYZYWOWY**

W projekcie przewidziano system przywoławczy. System przywoławczy SP umożliwia wezwanie pomocy, jeżeli osoba niepełnosprawna takiej potrzebuje.

Pociągnięcie za linkę przycisku pociągowego powoduje zadziałanie modułu alarmowego w korytarzu nad drzwiami wejściowymi do toalety dla niepełnosprawnych. Przyciski wzywający jest podświetlony światłem czerwonym i po wywołaniu alarmu sygnalizuje wysłanie wezwania. Alarm pozostaje aktywny do czasu skasowania sygnału, przyciskiem kasującym. Przycisk kasujący zamontować przy drzwiach wewnątrz pomieszczenia toalety dla niepełnosprawnych, na wysokości ok. 1,2m. Przyciski pociągowe montować na wysokości ok. 0,9 m od posadzki, przycisk montować powyżej poziomu poręczy. Moduł alarmowy w korytarzu montować nad drzwiami.

## **23. UWAGI KOŃCOWE**

- Całość prac wykonać zgodnie z obowiązującymi przepisami w ścisłej koordynacji z pracami innych branż.
- Dopuszcza się stosowanie materiałów zamiennych w stosunku do zamieszczonych w projekcie pod warunkiem, że parametry techniczne zamienników nie będą gorsze od parametrów urządzeń projektowanych.
- Przejścia przewodów przez strefy pożarowe należy zabezpieczyć masą ognioodporną o parametrach co najmniej równym klasie przegrody pożarowej przez którą prowadzona jest instalacja.
- Przy przejściu przewodów przez ściany i inne stałe elementy budowlane, należy chronić mechanicznie przewód ognioodporną rurą ochronną.
- Wykonać niezbędne badania i pomiary. Całość przekazać Inwestorowi.
- Należy stosować przewody oznakowane wg norm CPR.
- Należy stosować przewody zgodnie z normą N SEP-E-007:2017-09. Na drodze ewakuacyjnej klasy B2ca-s1b, d1,a1 . Poza drogami ewakuacyjnymi klasy Dca-s2, d1,a2

## OBLICZENIA TECHNICZNE

### 1. OBLICZENIE MOCY ZAINSTALOWANEJ I SZCZYTOWEJ

Proj. moc przyłączeniowa:  $P_p = 85 \text{ kW}$

$$I_s = \frac{85000}{\sqrt{3} \times 400 \times 0,93} = 132 \text{ A}$$

Zabezpieczenie przedlicznikowe  $I_B = 160 \text{ A}$ ,  
przewody złącze - tablica główna: 5xN2XH-J 1x95.

### 2. OBLICZENIE SPADKU NAPIĘCIA NA WLZ

Przenoszona moc  $P = 85 \text{ kW}$

przewody: Cu 95 mm<sup>2</sup> dł.  $l = 22 \text{ m}$ ,

$$\Delta U_{\%} = \frac{P \times l}{k \times s}$$
$$\Delta U_{\%} = \frac{85 \times 22}{83 \times 95} = 0,24\%$$
$$\Delta U_{\%} < \Delta U_{dop}$$

### 3. DOBÓR PRZEKŁADNIKÓW W UKŁADZIE POMIAROWYM

Dla układu pomiarowego projektuje się przekładniki prądowe 150/5A, kl. 0,2s o mocy  $S=5 \text{ VA}$ ,  $F_s=5$  i przeciążalności prądowej 120%  $I_n$ .

Znamionowy prąd strony pierwotnej przekładnika wynosi 150 A.

Prąd obliczeniowy dla mocy 85 kW wynosi 132A.

Obciążalność strony pierwotnej przekładników:

$$0,2I_n < I_{obl} < 1,2I_n$$

$$30 \text{ A} < 132 \text{ A} < 180 \text{ A}$$

Projektowane przekładniki mogą pracować w przedziale od 30A do 180 A prądu po stronie pierwotnej.

Obciążalność strony wtórnej przekładników:

Przekrój przewodów  $s=2,5 \text{ mm}^2 = 2,5 \cdot 10^{-6} \text{ m}^2$ ,

Konduktywność Cu  $\gamma=56 \cdot 10^6 \text{ S/m}$ ,

Długość obwodów wtórnych  $l=2 \text{ m}$ ,

Obciążenie od licznika  $Sl=0,125 \text{ VA}$ ,

Rezystancja styków  $Rz=0,05 \Omega$ ,

Prąd znamionowy strony wtórnej przekładników  $In2=5 \text{ A}$

$$Sobl = Sl + In2^2 \cdot \left( \frac{2 \cdot l}{\gamma \cdot s} + Rz \right) = 0,125 + 25 \cdot \left( \frac{2 \cdot 2}{56 \cdot 10^6 \cdot 2,5 \cdot 10^{-6}} + 0,05 \right) = 2,089 \text{ VA}$$

$$0,25Sn < Sobl \leq Sn$$

$$1,25 \text{ VA} < 2,089 \text{ VA} < 5 \text{ VA}$$

Projektowane przekładniki o mocy 5 VA spełnia warunki obciążalności strony wtórnej.

## **1. Zakres robót**

Wykonanie instalacji elektrycznych wewnętrznych obejmujących:

zasilanie i pomiar energii;  
tablice rozdzielcze i wewnętrzne linie zasilające;  
instalacje oświetlenia i gniazd wtykowych;  
instalację siły i zasilania odbiorników technologicznych;  
instalacje słaboprądowe;

## **2. Wykaz istniejących obiektów budowlanych**

- istniejące instalacje

## **3. Niebezpieczne elementy zagospodarowania terenu**

uzbrojenie podziemne, głębokie wykopy.

## **4. Przewidywane zagrożenia**

Podczas wykonywania prac mogą wystąpić następujące zagrożenia:  
niebezpieczeństwo związane z możliwością wystąpienia elementów instalacji elektrycznych znajdujących się pod napięciem;  
niebezpieczeństwa związane z koniecznością wykonywania prac na rusztowaniach i na drabinie;  
niebezpieczeństwa związane z koniecznością używania elektronarzędzi oraz możliwością niespodziewanego kontaktu z ostrymi przedmiotami.  
niebezpieczeństwa związane z koniecznością przebywania w pomieszczeniach zapyłonych.

## **5. Instruktaż pracowników przed przystąpieniem do realizacji robót**

Przed przystąpieniem do prac należy dokładnie przeszkolić pracowników odnośnie wykonywanych przez nich zadań.

W każdym zespole powinna być osoba posiadająca właściwe świadectwo kwalifikacyjne SEP.

## **6. Zapobiegawcze środki techniczne i organizacyjne**

Zabrania się wykonywania jakichkolwiek prac pod napięciem.  
Zabrania się stosowania niesprawnych narzędzi i urządzeń. Należy stosować wyłącznie narzędzia wyposażone w uchwyty z materiału izolacyjnego.  
Rozdzielnice budowlane muszą być wyposażone w wyłączniki różnicowo prądowe i uziemione.  
Zadbać o właściwy strój roboczy oraz odpowiednie przerwy w pracy.