

Wytyczne techniczne – SKD, CCTV, SSWIN oraz PSIM

Wersja 1.10 – 28.08.2026

1. Kontrola dostępu

Projektowany system kontroli dostępu ma za zadanie ograniczyć poruszanie się osób nieupoważnionych do przestrzeni ogólnodostępnej. Osoby upoważnione uzyskają dostęp do przestrzeni i pomieszczeń odpowiednio do pełnionej funkcji. Podstawą do wejścia do strefy chronionej będzie identyfikator w postaci karty zbliżeniowej. W celu minimalizacji prawdopodobieństwa wejścia osoby nieupoważnionej do strefy wydzielonej, każdy etap transmisji danych od karty do komputera będzie zabezpieczony poprzez szyfrowanie.

System KD pracować będzie jako beznapięciowo otwarty. Kontrolery systemu KD wyposażone będą w akumulatory zapewniające buforowanie zasilania (napięcie pracy 12V DC). Otwarcie przejść na drogach ewakuacyjnych realizowane poprzez zdjęcie napięcia z elektrozaczepów przy wykorzystaniu wyjść przekaźnikowych modułów wejść/wyjść systemu SSP.

W skład systemu KD wchodzić będą kontrolery główne, kontrolery drzwiowe, czytniki, elementy wykonawcze (elektrozaczepy, zwory elektromagnetyczne, przyciski wyjścia) oraz elementy sygnalizacyjne (kontaktrony). System KD zasilany będzie z dedykowanych zasilaczy, posiadających własne podtrzymanie bateryjne. Autoryzacja dostępu do pomieszczeń odbywać się będzie poprzez wykorzystanie, przez osoby upoważnione, szyfrowanych kart DESFire EV3.

System kontroli dostępu oparty zostanie o technologię Protege GX.

Ze względu na ograniczoną liczbę osób obsługujących wszystkie systemy bezpieczeństwa, system SKD musi umożliwiać integrację w systemie zarządzania SMS i stanowić spójną całość z pozostałymi zintegrowanymi systemami.

Ponadto wszystkie drzwi wewnętrzne do pomieszczeń należy zaprojektować w oparciu o system klucza generalnego (tzw. Master Key).

Wymagana jest integralność klucza systemowego Master Key z już istniejącym systemem w UAM, celem zwiększenia spójności w administrowanym obszarze. Kontrolery w obudowach należy umieszczać w pomieszczeniach objętych kontrolą dostępu. Dokładny projekt zawierający awers i rewers karty zostanie dostarczony do wykonawcy w późniejszym etapie prac. Czas podtrzymania pracy należy dobrać na podstawie bilansu energetycznego, jednak nie krótszy niż 8 godzin, chyba że Zamawiający określi inne wymagania w dokumentacji projektowej.

Poniżej zaprezentowano i opisano poszczególne składowe systemu KD:

PRT-CTRL-DIN Kontroler systemowy Protege GX, wersja DIN



Zaawansowany kontroler systemowy Protege GX to podstawowa jednostka sprzętowa odpowiedzialna za funkcje: kontroli dostępu, SSWiN, automatyki i innych. Komunikuje się ze wszystkimi modułami systemu, przechowuje całą konfigurację i informacje o zdarzeniach, przetwarza wszystkie procesy komunikacyjne systemu oraz raportuje alarmy i zdarzenia systemu do serwera.

Charakterystyczne cechy:

1. Port sieciowy Ethernet 10/100.
2. Port LAN.
3. Zaawansowany procesor RISC 32 Bit z całkowitą pamięcią 2Gb.
4. Szyfrowana sieć modułów wykorzystująca komunikację RS-485.
5. Szyfrowanie AES 128, 192 i 256-bit z certyfikatem NIST.
6. Wbudowany zewnętrzny dialer telefoniczny (ContactID, SIA).

2 porty czytników do obsługi dwóch przejść dwustronnych, niezależnie konfigurowalnych do pracy z czytnikami Wiegand lub RS-485.

1. Konfigurowalny protokół OSDP RS-485.
2. 8 monitorowanych wejść o wysokim poziomie bezpieczeństwa.
3. 2 wysokoprądowe wyjścia przekaźnikowe FORM C.
4. 1 wysokoprądowe nadzorowane wyjście sygnalizatora.
5. Frontowy panel z zestawami ikon informujących o stanie urządzenia.
6. Montaż na szynie DIN.

Zintegrowana kontrola dostępu zapewnia niezawodne rozwiązania kontroli dostępu klasy Enterprise.

7. Wiele poziomów dostępu do zarządzania użytkownikami w zaplanowanych harmonogramach.

8. Elastyczne zarządzanie użytkownikami dzięki przypisaniu grup drzwi, menu klawiatur, stref, pięter, wind do poziomu dostępu. Każdy użytkownik może być przypisany do kilku grup na różnych poziomach dostępu.

9. Monitorowanie i kontrola obszaru w całym systemie dzięki dwóm opcjom konfiguracji kontrolera:

APB Twardy i APB Miękki.

10. Wiele opcji prezentacji kart, breloków zbliżeniowych lub innych identyfikatorów do uzbrajania i rozbrajania stref z powiązanymi drzwiami.

11. Zliczanie osób wchodzących do strefy (również uzbrojonej), odmowa dostępu na podstawie funkcji maksymalnej dopuszczalnej liczby osób.

Łączność i rozbudowa systemu Protege jest łatwa i ekonomiczna:

12. 8 monitorowanych wejść na płycie głównej, z których każde można zaprogramować jako EOL, DEOL lub NC

13. 2 wysokoprądowe przekaźniki typu C

14. 2 zintegrowane porty czytników, niezależnie konfigurowalne do pracy w protokole Wiegand lub RS-485

15. Monitorowane wyjście syreny

16. Rozbudowa systemu odbywa się bezproblemowo poprzez podłączenie dodatkowych modułów

Zaawansowane funkcje programowania systemu Protege GX zapewniają nieskończone możliwości automatyzacji.

Funkcje programowalne to specjalne aplikacje, które umożliwiają zaawansowane sterowanie wyjściami, drzwiami, strefami i innymi urządzeniami.

PRT-RDM2-DIN-485 Kontroler 2 przejścia wersja DIN



Kontroler 2 przejść wersja MINI w obudowie DIN rozszerza funkcjonalność Zintegrowanego Kontrolera Systemowego PRT-CTRL-DIN o obsługę dodatkowych 2 przejść kontroli dostępu. Pozwala na podłączenie do 4 czytników w konfiguracji 2 przejść dwustronnych lub 2 czytników w konfiguracji 2 przejść jednostronnych. Kontroler PRTRDM2-DIN-485 to technicznie zaawansowane urządzenie, które zapewnia elastyczną rozbudowę systemu Protege GX.

Cechy charakterystyczne:

1. 2 porty czytnika konfigurowalne do obsługi czytnika Wiegand lub RS-485.
2. Konfigurowalny protokół OSDP RS-485.
3. 4 porty czytnika do obsługi dwóch przejść dwustronnych.
4. Zabezpieczone i monitorowane zasilanie czytnika.
5. Wsparcie dla technologii inteligentnej kontroli sabotaży czytnika, system monitoruje obecność czytnika za pomocą specjalnego protokołu.
6. Dostęp offline (w tym brak użytkowników, wszyscy użytkownicy i pierwszych 10 użytkowników oraz 150 kart w pamięci podręcznej).
7. Wbudowanych ponad 40 formatów odczytów.
8. Sterowanie do 3 wyjść na każdy port czytnika z wbudowanymi konfiguracjami do natychmiastowego podłączenia.
9. Frontowy panel z zestawami ikon informujących o stanie urządzenia.
10. Montaż na szynie DIN

Zintegrowane uzbrajanie/rozbrajanie umożliwia kontrolę wielu stref alarmowych:

11. Odmowa dostępu użytkownikom na podstawie statusu strefy, ale i również możliwości kontrolowania przez nich stref, do których wchodzi, co zmniejsza liczbę fałszywych alarmów.
12. Kontrola skarbców z funkcją opóźnionego dostępu i odblokowywaniem stref skarbców w obiektach bankowych.
13. Dostęp do klawiatury za pomocą karty i PIN w celu automatycznego zalogowania użytkownika.
14. Dostęp lub odmowa dostępu do wybranego piętra z poziomu windy na podstawie statusu strefy związanego z piętrem.
15. Uzbrajanie dużej liczby obszarów za pomocą grup stref.

Zasilanie

Kontroler wymaga zewnętrznego źródła zasilania 12VDC. Bardzo niski pobór prądu zapewnia małą ilość zasilaczy w systemie i efektywną dystrybucję zasilania.

Łączność oraz rozbudowa systemu.

Wejścia i wyjścia znajdujące się na kontrolerze pozwalają na swobodną, tanią, łatwą i efektywną rozbudowę systemu. Dodatkową zaletą jest podwójna funkcjonalność wejść monitorujących drzwi:

1. 8 wejść o wysokim poziomie bezpieczeństwa może być wykorzystywanych do monitorowania systemu, alarmowania oraz automatyki budynku. Wejścia posiadają wstępnie przypisane funkcje, które są przetwarzane przez kontroler w celu sterowania drzwiami. Każda funkcja może być aktywowana indywidualnie.
2. 6 wyjść typu otwarty kolektor może być wykorzystanych w systemie do zarządzania np. przekaźnikami, oświetleniem czy automatyką budynku.
3. Rozbudowa systemu przebiega bezproblemowo przez podłączenie dodatkowych modułów rozszerzeń.
4. Konfiguracja modułów rozszerzeń odbywa się za pomocą funkcji programowania adresów w kontrolerze.

Komunikacja

- Wbudowany port RS-485 wykorzystywany jest zarówno do komunikacji sieciowej jak również do komunikacji z pozostałymi modułami.

Czytnik zbliżeniowy DESFire 13.56MHz Standard Mullion, czarny



Czytniki TSEC Standard to kompletna seria czytników multi-technology smart card RFID. Czytniki posiadają interfejs Wiegand oraz możliwość komunikacji RS-485, dzięki czemu pozwalają na natychmiastowe wdrożenie bezpiecznej technologii w każdym środowisku, zarówno w nowych jak i istniejących już systemach. Czytniki TSEC odczytują karty różnych technologii (DESFire, Mifare i 125kHz), dostępne są w wersji z klawiaturą, a także w kolorze białym lub czarnym. Tak szeroki wybór pozwala na dopasowanie czytnika zarówno pod kątem technologii jak i designu. Do czytników można zastosować dodatkową obudowę nr ref. PRXSVRC.

Cechy charakterystyczne:

1. Wiele wspieranych technologii identyfikatorów zbliżeniowych DESFire, Mifare oraz 125kHz w jednym czytniku.
2. Odczyt zabezpieczonych kart DESFire EV1/EV2/EV3 i MIFARE.
3. Odczyt sektorów pamięci kart DESFire EV1/EV2/EV3 i MIFARE.
4. Dostępna wersja czytnika z klawiaturą PIN.
5. Elegancki wygląd wpasowuje się w każde wnętrze.
6. Czytniki dostępne w kolorze czarnym lub białym.
7. Połączenie RS-485 lub standard Wiegand.
8. Urządzenie całkowicie szczelne spełnia standard IP65 i może być zastosowane zarówno wewnątrz jak i na zewnątrz obiektów.
9. Dwukolorowa dioda LED (niebieska i zielona) z niezależnym sterowaniem oboma kolorami lub ze sterowaniem tylko jednym kolorem.
10. Zasięg do 60mm z kartami zbliżeniowymi ISO.

Wiele technologii zbliżeniowych

- Czytniki TSEC są dostępne w technologii 125kHz, smart card 13.56MHz lub jako czytniki multitechnology 125kHz + 13.56MHz w jednym czytniku, co zapewnia maksymalną kompatybilność z istniejącymi na obiekcie technologiami oraz możliwość łatwej integracji z najnowszymi bezpiecznymi technologiami. To sprawia, że czytniki serii TSEC są idealne dla organizacji, które chcą stopniowo zmieniać starsze technologie 125kHz na najnowsze i najbardziej bezpieczne technologie zbliżeniowe DESFire Mifare EV1.

Elastyczna komunikacja

- Wybieraj pomiędzy inteligentnym podłączeniem RS-485 dla szybkiej, elastycznej i bezpiecznej komunikacji lub połączeniem w standardzie Wiegand kompatybilnym z większością systemów dostępnych na rynku. RS-485 cechuje sposób okablowania i instalacji, co pozwala na bezpośrednią integrację w systemie Protege GX i dokonywanie zmian w samym czytniku w trakcie jego pracy. Magistrala RS-485 pozwala również na zastosowanie długich kabli i łatwiejszy proces aktualizacji firmware.

Klasa ochrony IP

- Stopień zabezpieczenia środowiskowego IP65 zapewnia odpowiednie zabezpieczenie w przypadku instalacji czytnika na zewnątrz budynków. Czytniki mogą być bez problemu stosowane zarówno wewnątrz jak i na zewnątrz budynków, od parkingów po drzwi w budynkach biurowych.

PRT-PSU-DIN-4A Inteligentny Zasilacz 12VDC/4A wersja DIN

Inteligentny zasilacz systemowy Protege 12VDC/4A wersja DIN dostarcza zasilanie dla urządzeń kontroli dostępu, systemu alarmowego, elementów automatyki oraz dużej liczby modułów systemu Protege. Zasilacz jest zaprojektowany w standardowej obudowie pozwalającej na łatwy montaż na szynie DIN. Zasilacz nie wymaga transformatora i jest bezpośrednio przyłączany do sieci 230VAC.

1. Bezpośrednie zasilanie z sieci 230VAC pozwala na szybką i łatwą instalację urządzenia.
2. 2 wyjścia zasilające 12VDC o łącznej obciążalności 4A.
3. 2 wyjścia przekaźnikowe Form B, które mogą być wykorzystane jako standardowe wyjścia programowalne dowolnego zastosowania w systemie Protege (jeżeli zasilacz jest online) lub jako wyjścia sygnalizujące status baterii i sieci AC, kiedy zasilacz jest w trybie offline.
4. Podłączenie akumulatora pozwalające na zasilanie urządzeń, kiedy sieć AC jest niedostępna.
5. Inteligentne algorytmy ładowania i monitorowania akumulatora oraz zasilania AC zwiększają funkcjonalność urządzenia.
6. Komunikacja z systemem Protege za pośrednictwem magistrali RS-485.

7. Ładowanie i kontrola akumulatora za pomocą mikroprocesora.
8. Zasilacz pracuje jako moduł zasilający w sieci modułów Protege i jego status jest ciągle monitorowany przez system.
9. Wartości napięć i poborów prądu są monitorowane w systemie Protege i mogą być prezentowane w wartościach analogowych np. na mapach wizualizacji.
10. Przekroczenie wartości progowych parametrów pracy zasilacza może powodować występowanie alarmów i ostrzeżeń w systemie Protege.
11. Urządzenie pracuje pod kontrolą zaawansowanego mikroprocesora 32 Bit.
12. Urządzenie w standardowej obudowie DIN.

Ekspandery linii PRT-IO84-DIN



Ekspandery PRT-IO84-DIN – 8 wej, 4 wyj. Moduł rozszerzenia umożliwia podłączenie do 8 wejść i sterowanie 4 wyjściami przekaźnikowymi FORM C w systemie Protege. Zaawansowane rozwiązania sprzętowe umożliwiają elastyczne programowanie i konfigurowanie wejść oraz sterowanie np. oświetleniem i automatyką budynkową.

Cechy charakterystyczne:

13. Podłączenie dowolnej kombinacji linii alarmowej NC lub NO, w tym z rezystorami EOL, konfigurowalne dla każdego wejścia osobno.
14. Przetwarzanie analogowo/cyfrowe z pięciokrotnym nadpróbkowaniem.
15. 4 stany wejścia alarmowego przy wykorzystaniu rezystorów końca linii (zamknięta, otwarta, sabotaż, zwarcie).
16. 4 przekaźniki FORM C 7A/250V.
17. Wydajny procesor 32-bity.
18. Frontowy panel z zestawami ikon informujących o stanie urządzenia.
19. Montaż na szynie DIN.

Zasilanie

Moduł wymaga zewnętrznego źródła zasilania 12VDC. Bardzo niski pobór prądu zapewnia małą ilość zasilaczy w systemie i efektywną dystrybucję zasilania.

IN-BOXDIN4 Obudowa dla urządzeń systemu Protege na szynę DIN



Metalowa obudowa IN-BOXDIN4 jest zaprojektowana specjalnie dla modułów systemu Protege wykonanych w formie urządzeń do montażu na szynę DIN. Obudowa posiada zamontowane dwa rzędy szyny DIN pozwalające na montaż maksymalnie 4 modułów Protege DIN.

Obudowa jest wyposażona w:

1. Szyny DIN do montażu maksymalnie 4 modułów Protege DIN.
2. Styk antysabotażowy otwarcia obudowy.
3. Styk antysabotażowy oderwania obudowy od ściany.
4. Zamek.

UWAGA – zaprojektowany i wykonany system kontroli dostępu może zostać uruchomiony dopiero po dostosowaniu obiektu do aktualnie obowiązujących przepisów dotyczących ochrony przeciwpożarowej oraz objęciu całego budynku systemem sygnalizacji pożaru SSP. Zamki elektryczne zamontowane w drzwiach objętych kontrolą dostępu do czasu połączenia z automatyką systemu sygnalizacji pożaru, zwalniającą drzwi w trakcie alarmu pożarowego muszą pozostać niepodłączone do napięcia. Po zintegrowaniu systemu kontroli dostępu z systemem automatyki pożarowej SSP należy przeprowadzić próby odbiorcze potwierdzające prawidłowe współdziałanie niniejszych systemów.

W przypadku lokalizacji szaf teletechnicznych w korytarzach lub pomieszczeniach, które nie mogą zostać objęte systemem kontroli dostępu, drzwi szaf należy zabezpieczyć poprzez zastosowanie kontroli dostępu, wyposażonej co najmniej w czytnik oraz elektrozamek.

Przewód komunikacyjno-zasilający do czytników ICT RS-485 / OSDP

Do połączenia kontrolerów, ekspanderów oraz czytników systemu kontroli dostępu ICT Protege GX należy stosować dedykowany przewód typu **RS-485 /OSDP Access Control Cable** lub przewód równoważny o parametrach nie gorszych niż podane poniżej

Parametr	Wymaganie
Zastosowanie	Połączenie kontrolerów, ekspanderów i czytników systemu kontroli dostępu ICT Protege GX pracujących w standardzie RS-485 / OSDP.
Przewody zasilające	2 × 18 AWG (ok. 0,82 mm ²), żyły wielodrutowe cynowane (TC).
Kolory żył zasilających	Czerwony (+), Czarny (-).
Przewody transmisyjne	1 para skręcana ekranowana 24 AWG do transmisji RS-485/OSDP.
Kolory żył transmisyjnych	Żółty, Fioletowy.
Ekran	Folia AL/PET z przewodem drenażowym (drain wire).
Impedancja charakterystyczna	120 Ω ±15%.
Maksymalne napięcie pracy	300 V.
Powłoka zewnętrzna	PVC, kolor biały.
Średnica zewnętrzna kabla	Okolo 6 mm.
Temperatura pracy	Od -20°C do +75°C.
Norma kabla komunikacyjnego	UL444.
Klasa odporności ogniowej	CMR / FT4.
Maksymalna długość magistrali RS-485	Do 1200 m przy zachowaniu zasad prowadzenia magistrali RS-485.
Topologia magistrali	Liniowa (daisy chain), bez połączeń gwiazdowych.
Terminacja magistrali	Rezystory EOL 330 Ω na pierwszym i ostatnim urządzeniu magistrali RS-485.

Ekranowanie	Ekran przewodu należy uziemić jednostronnie w szafie teletechnicznej / rozdzielni.
Zalecenie dla odległości >200 m	Zaleca się stosowanie lokalnego zasilacza przy przejściu oraz wykorzystanie magistrali RS-485 wyłącznie do transmisji danych. <i>(zalecenie projektowe)</i>

Dla wszystkich nowych instalacji czytniki systemu KD należy podłączać z wykorzystaniem protokołu OSDP realizowanego po magistrali RS-485. Stosowanie transmisji Wiegand dopuszcza się wyłącznie w przypadku modernizacji istniejących instalacji, gdy nie ma możliwości zastosowania OSDP.

Okablowanie systemu KD

Element	Minimalne wymaganie
Czytnik – kontroler	Dedykowany przewód RS-485/OSDP wg wymagań niniejszej specyfikacji
Kontaktron	YTDY 6×0,5 mm ² lub równoważny
Przycisk wyjścia	YTDY 4×0,5 mm ² lub równoważny
Zwora / elektrozaczep	YLY lub OMY 2×1,0 mm ² lub wg obliczeń spadku napięcia
Magistrala modułów Protege	Dedykowany przewód RS-485 ekranowany 120 Ω
Ethernet do kontrolerów systemowych	Kat. 6A F/UTP lub lepsza

2. SSWIN

Ekspandery linii PRT-IO84-DIN



Ekspandery PRT-IO84-DIN – 8 wej, 4 wyj.

Moduł rozszerzenia umożliwia podłączenie do 8 wejść i sterowanie 4 wyjściami przekaźnikowymi FORM C w systemie Protege. Zaawansowane rozwiązania sprzętowe umożliwiają elastyczne programowanie i konfigurowanie wejść oraz sterowanie np. oświetleniem i automatyką budynkową.

Cechy charakterystyczne:

1. Podłączenie dowolnej kombinacji linii alarmowej NC lub NO, w tym z rezystorami EOL, konfigurowalne dla każdego wejścia osobno.
2. Przetwarzanie analogowo/cyfrowe z pięciokrotnym nadpróbkowaniem.
3. 4 stany wejścia alarmowego przy wykorzystaniu rezystorów końca linii (zamknięta, otwarta, sabotaż, zwarcie).
4. 4 przekaźniki FORM C 7A/250V.
5. Wydajny procesor 32-bity.
6. Frontowy panel z zestawami ikon informujących o stanie urządzenia.
7. Montaż na szynie DIN.

Zasilanie

Moduł wymaga zewnętrznego źródła zasilania 12VDC. Bardzo niski pobór prądu zapewnia małą ilość zasilaczy w systemie i efektywną dystrybucję zasilania.

Klawiatura dotykowa LCD do systemu PROTEGE (biała)



Dotykowa Sensoryczna Klawiatura LCD PRT-KLCS jest nowoczesnym i przyjaznym dla użytkownika interfejsem obsługi systemu Protege, który jest zaawansowanym systemem

zarządzania bezpieczeństwem integrującym kontrolę dostępu, SSWiN, CCTV, automatykę budynku i inne systemy.

Cechy charakterystyczne:

1. Elegancka i stylowa klawiatura dotykowa PRT-KLCS pasuje do nowoczesnego wystroju wnętrz oraz zapewnia przyjazny dla użytkownika interfejs do obsługi Zintegrowanego Systemu Bezpieczeństwa i Automatyki Budynku Protege.
2. Bezpieczne logowanie za pomocą kodu użytkownika od 1 do 8 cyfr z możliwością integracji z czytnikami kart, a także z możliwością logowania kombinacjami kodów master/slave (podwójny kod).
3. Intuicyjne menu z funkcjami przewijania, dopasowane do każdego użytkownika, z funkcjami ograniczonymi przez poziom dostępu, z klawiszami szybkiego dostępu.
4. Funkcje logowania dwoma kodami i/lub kodem master/slave, z opcjami automatycznego upływu czasu oraz z opóźnionego rozbrojenia, zapewniają niedościgniony poziom bezpieczeństwa dla stref o najwyższym stopniu zabezpieczenia.
5. Pojemnościowa klawiatura dotykowa.
6. Indywidualne kody raportowania problemów i przymusu dla każdej klawiatury.
7. Aktywacja 3 raportowalnych zdarzeń nagłych (napad, alarm medyczny i pożar) za pomocą przycisków bezpośredniego dostępu.
8. Reset czujek pożarowych za pomocą przycisków CLEAR i ENTER, z możliwością uruchomienia wyjścia PGM lub grupy wyjść.
9. Klawiatura dostępna w kolorze czarnym.

Czujka IR 918AM

Czujka IR 918AM do wykrywania ruchu wykorzystuje technikę mikroprocesorową oraz cyfrową obróbkę sygnału. Posiada zabezpieczenie przed zastąpieniem soczewki – tzw. antymasking. Czujka posiada

podwójny filtr przeciwwzakłóceńowy, eliminujący wpływ obcego pola elektromagnetycznego.

Dla właściwej pracy toru podczerwieni w trudnych warunkach przewidziany jest licznik impulsów oraz możliwość wyboru impulsu bipolarnego lub quad. Czujki montowane będą na uchwytych sufitowych/ściennych typu SP900

Dane techniczne czujki IR 918 AM:

1. Napięcie zasilania od 9 do 15VDC
2. Pobór prądu praca/alarm 25 mA / 32mA (włączona LED)
3. Zasięg działania 18 m (soczewka szerokokątna)
25 m (soczewka dalekiego zasięgu)
1. Wymiary 138 x 74 x 53 mm
2. Temperatura pracy od -10 °C do 55 °C

3. CCTV

Dla opcji rejestracji lokalnej i możliwości przesyłania obrazu do centrum zarządzania VDG Sense w Poznaniu przyjęto następujące parametry i wymogi dotyczące optymalizacji zasobów:

Wielostrumieniowość – optymalizacja zasobów.

System musi dawać możliwość zaawansowanego zarządzania strumieniami tzw. wielostrumieniowość, z pobieraniem jednocześnie z kamery minimum trzech różnych strumieni video z możliwością dowolnego przypisania każdego ze strumieni do wskazanego zadania: zapisu video, analizy obrazu (VCA, detekcja ruchu, LPR itd.) lub podglądu video z wykorzystaniem trzech stopni podglądu w zależności od wielkości siatki definiowanej przez szerokość panelu, który może być skonfigurowany w zakresie minimum od 1 do 1080 pikseli np.:

- | | |
|-------------------------|---|
| 1. Podgląd 1x1 kamery | - strumień 1szy rozdzielczość 4K, 12 kl./s |
| 2. Podgląd 2x2 kamery | - strumień 2gi rozdzielczość FullHD, 20 kl./s |
| 3. Podgląd 3x3/4x4 itd. | - strumień 3ci rozdzielczość D1, 25 kl./s |

Podczas wyświetlania w widoku wielokamerowym podglądu na żywo, klient systemu powinien automatycznie wybrać opcję wyświetlania jednego z trzech strumieni obrazu wideo o niższej jakości, ze źródła wideo, zgodnie z rozmiarem panelu podglądu na żywo, ustawionego przez użytkownika. Obraz automatycznie przełączy się na wyświetlanie obrazu wideo o najwyższej rozdzielczości (HD), gdy operator wybierze wyświetlanie na pełnym ekranie podglądu obrazu na żywo. Ma to na celu utrzymanie najlepszej i najbardziej wydajnej pracy procesora oraz zarządzanie obciążeniem sprzętu, które zapewniają wyświetlanie wszystkich obrazów wideo z płynnym ruchem bez opóźnień, zapewniając podgląd minimum 120 kamer jednocześnie.

Każdy ze strumieni video będzie mógł być konfigurowany w zakresie minimum poniższych parametrów:

4. Jakości obrazu - wymagana gradacja minimum 1000 poziomów jakości
5. Rozdzielczość - tyle wariantów, ile zapewnia kamera dla strumienia
6. Ilości klatek - tyle wariantów, ile zapewnia kamera dla strumienia • Typu transmisji: unicast lub multicast

Zmiana parametrów dowolnego z trzech strumieni musi być możliwa do wykonania ręcznie, z panelu administratora, widoków, przycisków, poligonów na mapach udostępnionych operatorom oraz dynamicznie, z wykorzystaniem silnika makr w efekcie reakcji na wcześniej

skonfigurowane reguły zachowania. Funkcjonalność zapewnia olbrzymią elastyczność systemu oraz eliminację tzw. wąskich gardeł w infrastrukturze klienta.

Ponadto dla strumienia przeznaczonego dla zapisu video system musi zapewniać możliwość zapisu rozrzedzonego tzw. migawkowego z interwałem czasowym w zakresie minimum 1- 999999999 sekund. Zapewni to możliwości wykonania time-laps`ów oraz gwarancje zapisu niezależnie, np. od działania analizy detekcji ruchu w kamerze.

Obsługa operatorska – system musi zapewniać nieograniczoną licencyjnie ilość jednoczesnych połączeń klienckich z komputerów zdalnych wyposażonych w aplikacje kliencką systemu, urządzeń mobilnych obsługiwanych przez system Android lub iOS oraz z przeglądarki internetowej.

Ze względu na wrażliwe dane jakimi będą nagrania, system nie powinien umożliwiać operatorom dowolnego eksportu i kopiowania nagrań. Eksport i kopiowanie nagrań powinno być możliwe tylko w przypadkach uzasadnionych i powinno być autoryzowane przez dwóch użytkowników systemu, a mianowicie operatora i administratora (kierownika) przez tzw. Funkcjonalność dualnego logowania.

System musi zapewniać możliwość importu użytkowników do systemu z usług katalogowych systemu min. Active Directory i LDAP oraz wykorzystanie mechanizmów jednorazowego logowania do systemu tzw. SSO.

Ponadto system musi posiadać moduł umożliwiający wykonanie audytu działań operatora z poziomem szczegółowości umożliwiającym weryfikację każdego działania na interfejsie min. dokładnego momentu eksportu kamer, zakresu eksportu materiału video, wyzwalanie makr, wybór kamer do podglądu video, przełączanie widoku, wyzwolenie przekaźnika w kamerach itd. Dane o działaniach muszą być przetrzymywane w bazie danych systemu VMS z możliwością filtrowania po nazwie użytkownika, stanowiska na jakim użytkownik się logował oraz działań, które były wykonywane. Każde działanie odkładane jest jako zdarzenie na liście zdarzeń w bazie danych. Wszystkie zdarzenia mogą podlegać reakcji przez makro – np. wysłanie e-mail'a do administratora w przypadku eksportu materiału

System musi umożliwiać wyznaczenie limitu z dokładnością do godziny dostępu do materiału video dla operatora, czyli np. operator może mieć dostęp do materiału video nie starszego niż 5 godzin.

Dostosowany do użytkownika widok powinien odnosić się do graficznego interfejsu użytkownika („GUI”), który sam jest tworzony przez użytkownika lub administratora systemu. Widok operatora umożliwia mieszanie i umieszczanie dowolnej liczby i rozmiaru panelu podglądu na żywo, panelu odtwarzania, panelu alarmów i zdarzeń, panelu mapy, panelu podglądu zdarzeń na żywo, panelu zegara, licznik w ramach tego samego GUI zgodnie z wymaganiami operatora. Nie może być ograniczeń co do tego, jak użytkownik chce, aby wyglądał jego układ.

System powinien zapewniać elastyczność pozwalającą na wyświetlanie pojedynczego widoku lub układu widoku na wielu monitorach, aby przełączyć się na kompletny, inny układ za pomocą jednorazowej akcji, ręcznie lub automatycznie w oparciu o alarm lub zdarzenia.

1. w pełni edytowalne przyciski ekranowe rozmieszczane w dowolnym miejscu poszczególnych widoków, zapewniające możliwość przełączenia pomiędzy widokami lub wyzwalania zaawansowanych makr oferujących możliwość wielopoziomowych akcji, w tym min wysterowanie presetów kamery PTZ, aktywacja wyjścia przekątnikowego w kamerze, nadanie uprawnień rozpoznania tablic rejestracyjnych dla danej kamery, sterowanie modułami
2. aktywowanie dowolnego makra w tym presetów kamer PTZ po kliknięciu kursorem myszy na predefiniowanym transparentnym regionie obrazu na dowolnym widoku powiązanej kamery stacjonarnej,
3. zaawansowane zbliżenia cyfrowe – możliwość zbliżenia cyfrowego dla wielu fragmentów z danej kamery, jednocześnie przy możliwości zachowania podglądu na całą obserwowaną przez nią scenę
4. jednoczesny podgląd obrazu archiwalnego z minimum 48 kamer w jednym widoku
5. jednoczesny podgląd obrazu na żywo z minimum 100 kamer na jednej stacji operatorskiej i nieograniczonej liczby kamer w trybie videowall
6. swobodne nadawanie przez administratora systemu hierarchicznych uprawnień każdemu operatorowi lub grupie operatorów korzystających z odpowiednich dla nich zasobów systemu, takich jak dostęp grup użytkowników do urządzeń, funkcjonalności urządzeń, widoków, reguł makr domyślnego widoku wyświetlanie
7. edytowalne reguły makr budowane w oparciu o instrukcje warunkowe aktywowane krzyżowo przez wszelkie zasoby oraz funkcjonalności systemu (np. rozpoznanie tablicy rejestracyjnej z tzw. białej listy automatycznie aktywuje przełączenie widoku na ekranie monitora oraz otworenie bramy wjazdowej do garażu)
8. wsparcie 8 i więcej monitorów o dowolnej przekątnej ekranu w ramach każdego stanowiska operatorskiego, w tym wirtualnego kontrolera z matrycą dotykową oraz klawiaturą numeryczną
9. obsługa funkcji tzw. videowall z możliwością zdalnego delegowania zawartości poszczególnych widoków, wyświetlanych na ekranach monitorów podrzędnych stacji operatorskich
10. wybór kamery do aktualnego podglądu przez przeciągnięcie ikony kamery z mapy synoptycznej lub mapy Geo wskazującego dokładną lokalizację geograficzną (wyrażoną w danych GPS) danej kamery
11. wskazanie materiału blokowanego przed nadpisaniem

12. możliwość doboru czasu nagrania dla każdej z kamer indywidualnie
13. zmiana atrybutów zapisu przypisana do aktywnego profilu
14. odtwarzanie ostatnich kilkunastu sekund nagrania, bezpośrednio z widoku kamery będącej aktualnie w trybie podglądu bieżącego obrazu, po kliknięciu prawym przyciskiem myszy
15. dynamiczna zmiana trybów, parametrów nagrywania poprzez makra jako reakcja na dowolne zdefiniowane przez użytkownika zdarzenie w systemie
16. zmiana parametrów nagrywania w oparciu o kalendarz tygodniowy lub roczny, dedykowane szczególnie dla wydarzeń niepowtarzalnych w terminarzu jak imprezy masowe
17. eksport materiału z wielu serwerów jednocześnie do jednego pliku z materiałem archiwalnym
18. eksport zdjęć z danego kadru musi umożliwiać operatorowi wskazać wycinek obrazu, który będzie eksportowany, zapis w formacie plików oraz wykonać korektę ustawień gammy, poziomu czerni i bieli
19. eksport materiału video musi być możliwy do min. dwóch formatów:
producenckim, zapewniającym największe bezpieczeństwo i szyfrowanie danych oraz ogólnodostępnym jak MP4 wraz z metadanymi dotyczącymi min. analizy obrazu i wskazaniem występowania obiektów tzw. BLOB
20. system musi zapewniać moduł zrzutu zdjęć z kamery we wskazane miejsce, w przypadku utraty połączenia pomiędzy serwerem a kamerą lub dezaktywacji kamery w serwerze
21. oprogramowanie zapewnia możliwość planowania kopii zapasowych z nagraniami wideo i zdarzeniami do folderu lokalnego lub na zmapowany dysk sieciowy z możliwością automatycznego kasowania najstarszych kopii zapasowych w przypadku wyczerpania się miejsca do zapisu nowych kopii zapasowych. Moduł ten umożliwia automatyczny odroczone w czasie eksportu danych wideo z wybranej kamery lub kamer. Musi istnieć możliwość wyboru przedziału czasowego (z dokładnością do 1 sekundy) archiwizowanego/eksportowanego materiału, czasu uruchomienia automatycznej archiwizacji lub eksportu (z dokładnością do 1 sekundy), formatu eksportu (natywny lub MP4) i docelowego miejsca eksportu
22. obsługa kamer 360 stopni typu rybie oko – odbywa się przez możliwość rozłożenia jednego strumienia kamery dowolnego producenta na trzy widoki w dedykowanych panelach umożliwiających: podgląd panoramiczny, sferyczny oraz podgląd na obszar wybrany przez obrót ePTZ i przez wskazanie przez operatora w podglądzie panoramicznym oraz sferycznym, przy czym obserwowany na tym panelu obraz jest zaznaczany obwódką w celu łatwej orientacji w obserwowanym

materiale. Przetwarzanie kamer typu rybie oko musi być certyfikowane przez Immervision Enables®

23. możliwość precyzyjnej lokalizacji zdarzenia na skorelowanej mapie synoptycznej np. poprzez wskazanie przez podświetlenie transparentnych wielopolygonowych obszarów, wizualizujących miejsce wykrycia alarmu.
24. możliwość korelacji dowolnej reakcji systemu np. przełączenie trybu nagrywania, wyzwolenie presetów kamery, przesłanie sygnału do systemu integrowanego, aktywacja analizy obrazu dla wybranej kamery lub grupy kamer, wyzwalanego poprzez transparentny wielopolygonowy obszar
25. możliwość wysłania emaila z dołączanym zdjęciem prezentującym zdarzenie alarmowe, poprzez wykorzystanie silnika makr wraz z możliwością tworzenia generycznych makr – przechwytywanie wielu zdarzeń przez jedno generyczne makro
26. alarmowanie o opóźnieniach w transmisji materiału z kamer – jest kluczowe w systemach wykorzystujących punkty kamerowe do: sterowania automatyką/weryfikacji procesów technologicznych, obsługi systemów rozproszonych. System musi alarmować operatora w przypadku wystąpienia opóźnień w transmisji obrazu powyżej 500 ms. System musi zapewniać operatorowi jasny komunikat np. czerwony krzyż oraz możliwość obsłużenia zdarzenia poprzez silnik makr
27. komentarze operatora (bookmark) - w przypadku wystąpienia sytuacji alarmowej np. wykrycie intruza przez analizę obrazu na kamerach termowizyjnych, realizujących wirtualną ochronę obwodową, system wygeneruje u operatora automatycznie widok, gdzie operator będzie musiał wpisać odpowiednią notatkę dotyczącą zdarzenia z możliwością wskazania, aby materiał ten został zablokowany przed nadpisaniem. Administrator lub operator nadrzędny będzie miał możliwość bardzo szybkiego wyszukania zabezpieczonego zdarzenia, przez wyszukanie odpowiednich fraz komentarza, w bazie danych systemu CCTV lub przez wyszukanie komentarza na linii czasu odtwarzania materiału video czy liście zdarzeń systemu pojawiającej się w interfejsie. Dodatkowo operator ma również możliwość dodawania swoich komentarzy i wskazania materiału do zablokowania przed nadpisaniem, dla dowolnego wydarzenia wskazanego przez niego ręcznie na linii czasu odtwarzania materiału lub dla kamery z podglądem na żywo, przez wskazanie kamery i wciśnięcie przycisku generującego makro wyświetlające widok dodawania komentarza
28. linia odtwarzania materiału video zapewnia operatorowi możliwość szybkiego wyszukiwania zdarzeń, dzięki podglądowi miniatur zdjęć ostatnich klatek w przód oraz w tył, w stosunku do wskazanego momentu na linii czasu, wskazanie graficznie ilości ruchu oraz graficzną reprezentację występujących zdarzeń wygenerowanych przez wejścia audio kamer, rozłączenie, połączenie kamer,

analizy tablic rejestracyjnych, analizy twarzy, detekcji twarzy, detekcji koloru, zakładek z komentarzem operatora oraz innych zdarzeń występujących w systemie VMS za pomocą prążków, po najechaniu na który pojawia się zdjęcie z momentu wystąpienia zdarzenia wraz z opisem danego zdarzenia, np. nr rozpoznanej tablicy, opis wykrycia itp.

29. interfejs operatora musi zapewniać możliwość tworzenia makr wywoływanych za pomocą przycisków w widokach, które umożliwiają zmiany wszystkich dostępnych parametrów urządzeń za pomocą HTTP/API dowolnych urządzeń min. zmiana adresu IP kamery, włączenie/wyłączenie analizy obrazu wbudowanej w kamerze, włączenie/wyłączenie funkcji WDR, HLC, masek prywatności, reset urządzenia, wyzwolenie przekaźnika w kamerze, interkomie, module wejść/wyjść, za zbrojenie stref SSWiN, KD w systemach trzecich np. kontrola interkomów SIP, sterowanie automatyką w sieci IP i wiele innych. Funkcjonalność ta musi zapewniać możliwość komunikowania się z urządzeniami za pomocą metod DELETE, GET, PUT, POST, UPDATE itp. z autoryzacją lub bez.

30. możliwość wskazania priorytetów zdarzeń przez wskazanie dla każdego z typu zdarzeń (detekcja ruchu, sabotaż, LPR, detekcja twarzy itd.) indywidualnego koloru z palety minimum 255 kolorów, które są przypisane do wystąpienia zdarzeń na liście zdarzeń oraz linii czasu. Szablony kolorów muszą być możliwe do przypisania do wybranej grupy operatorów. Funkcjonalność

zapewnia wysoką ergonomię pracy oraz bardzo szybką możliwość orientacji sytuacyjnej.

31. możliwość nakładania masek prywatności na kamerze z poziomu interfejsu graficznego VMS. Minimum 8 masek ze wskazaniem jej wielkości, miejsca w scenie oraz indywidualnego nazwania każdej z masek

Dodatkowe moduły, integracje, API/SDK systemu

W ramach budowy systemu lokalnego VDG Sens należy przewidzieć rozbudowę licencji głównej o moduł komunikacji API. Ma to na celu możliwość podłączenia systemu VMS do pozostałych komponentów techniki zabezpieczeniowej, aby uzyskać spójny i wydajny system informowania o zagrożeniach wraz z dostępem do nagrań z obiektów wyniesionych.

Integracja z systemami trzecimi min BMS, SMS itd., musi zapewniać komunikację z dowolnym systemem trzecim w tym z systemami zarządzania bezpieczeństwem, budynkami SMS, BMS, PSIM na bazie interfejsu API/ HTTP obsługiwanego przez protokół TCP/IP, który umożliwia integrację dwukierunkową o następujących funkcjonalnościach:

1. przełączanie widoków oraz multi-widoków w systemie CCTV IP w wyniku detekcji alarmu w dowolnym systemie obsługiwanym przez system nadrzędny BMS

2. przełączanie widoków oraz multi-widoków w systemie CCTV IP w wyniku detekcji alarmu w dowolnym systemie. Zgodnie z zapisami ekspertyzy technicznej sygnał alarmowy z centrali SSP będzie przekazany poprzez system integrujący PSIM WinGuard do serwera VDG co spowoduje na stacji poglądowej w portierni generację obrazów z kamer obszaru objętego pożarem
3. zdalne kontrolowanie funkcji kamer PTZ
4. zdalne kontrolowanie makr systemu CCTV w celu umożliwienia wielopoziomowych predefiniowanych reakcji na zdarzenia zaistniałe w systemie nadrzędnym lub systemach przez niego kontrolowanych
5. generowanie zdarzeń w bazie danych systemu CCTV z przypisaniem powiązanego obrazu z danej kamery, w celu możliwości wyszukania informacji w bazie danych z wykorzystaniem metadanych o danym zdarzeniu, przez wpisanie części lub pełnego opisu alarmu
6. import zdarzeń będących wynikiem działania algorytmów analizy obrazu
7. wyświetlanie obrazu z kamer w trybie bieżącego podglądu, jak również odtwarzanie materiału archiwalnego w wizualizacji systemu nadrzędnego
8. wskazywanie materiału to tzw. tagowanie, czyli blokowanie materiału przed nadpisaniem
9. generowanie komentarzy w systemie VMS tzw. bookmark, które są widoczne na linii czasu oraz w bazie danych
10. możliwość eskalowania zdarzeń i dzielenia się komentarzami oraz przekazywanie zdarzeń między operatorami systemu VMS oraz nadrzędnego
11. dostarczanie przez system VMS strumieni RTSP (minimum H.265/H.264) z dynamicznym wyborem minimum trzech różnych strumieni, w zależności od wielkości okna z podglądem video wyświetlanego przez system integrujący– funkcja zapewnia znaczną optymalizację obciążenia sieci LAN oraz obciążenia stacji operatorskich SMS/PSIM umożliwiając wyświetlanie maksymalnej ilości kamer

Wytyczne odnośnie do kamer:

Kamera IP zewnętrzna typu **bullet**, o parametrach nie gorszych niż:

- rozdzielczość 2592x1944,
- przetwornik min. 1/2.8"
- mechaniczny lub automatyczny filtr podczerwieni,
- kompresja H.265,
- obiektyw o zmiennej ogniskowej 2,7-13,5mm,

- wbudowane diody IR – zasięg do 50m,
- klasa szczelności IP67,
- obudowa wandaloodporna IK10,
- bitrate konfigurowalny, min. Do 8Mb/s dla 5 Mpix,
- obsługa CBR/VBR
- zasilanie 12Vdc/PoE,
- wbudowane gniazdo pamięci SD/SDHC/SDXC – 256G;
- funkcje: maski prywatności, BLC, HLC, 2D DNR, 3D DNR, ROI, Defog, AWB, EIS, IP Address Filtering, AGC, filtr migotania, tryb korytarzowy, Deblur, znak wodny, VoIP, ONVIF: profile G & Q & S & T
- zaawansowana analiza obrazu.

Kamera IP wewnętrzna **kopułkowa**, o parametrach nie gorszych niż:

- rozdzielczość 2592x1944,
- mechaniczny lub automatyczny filtr podczerwieni,
- przetwornik min. 1/2.8"
- kompresja H.265,
- obiektyw o zmiennej ogniskowej 2,8-8,4mm,
- wbudowane diody IR – zasięg do 35m,
- klasa szczelności IP66,
- obudowa wandaloodporna IK10,
- zasilanie 12Vdc/PoE,
- wbudowane gniazdo pamięci SD/SDHC/SDXC – 256G,
- wbudowany mikrofon,
- bitrate konfigurowalny, min. do 8 Mb/s dla 5 Mpix
- obsługa CBR/VBR
- funkcje: maski prywatności, BLC, HLC, 2D DNR, 3D DNR, ROI, Defog, AWB, EIS, IP Address Filtering, AGC, filtr migotania, tryb korytarzowy, Deblur, znak wodny, VoIP, ONVIF: profile G & Q & S & T.
- zaawansowana analiza obrazu.

Serwer systemu CCTV o parametrach nie gorszych niż:

Parametry techniczne	
Chipset	Intel C256
Karta graficzna	Aspeed AST2600 64MB VRAM (VGA) (Wbudowana)
Interfejs sieciowy	2 x 1GbE LAN + 1 x Mgmt LAN (działa w połączeniu z NVH-RMMv2), Kontroler LAN obsługuje 100Base-T, 1000Base-T
Płyta główna	P12R-E
Kontroler RAID	Kontroler RAID SAS i SATA 12 Gb/s
TPM - moduł szyfrowania	TPM 2.0
RMM - moduł zdalnego zarządzania	Asus ASMB10-iKVM
Sieć LAN	2 x Intel® I210AT + 1 x Mgmt LAN
Procesor	Intel Xeon E2300
Wydajność	64-bitowa architektura, 700 Mbit/s, do 320 kamer FullHD
Zgodność	Zgodność z sekcją 889 NDAA
Dysk twardy	Dysk SSD NVMe 512 GB (w zestawie)
Pamięć RAM	16 GB
Wyjście wideo	VGA
Wydajność CPU	Powyżej 16 000 pkt wg CPU Benchmark
System operacyjny	Microsoft Windows 11 Pro 64-bit
Konfiguracja RAID	Standardowa konfiguracja Raid 5 (opcje konfiguracji RAID: 0, 1, 5, 6, 10 i hot-spare)

Diagnostyka	Funkcjonalność monitorowania i alarmowania o anomaliach on-line urządzeń sieciowych (przy wykorzystaniu platformy VDG Sense)
Parametry zasilania	
Zasilanie	100-240VAC, 50 / 60Hz 5A
Pobór mocy	200 W
Zasilacz	400W Pojedynczy
Parametry środowiskowe	
Temperatura pracy	Od +10°C do +50°C
Temperatura przechowywania	od -40°C do +70°C
Parametry mechaniczne	
Wymiary	550 x 438.5 x 43.2 mm
Forma urządzenia	19-calowy o wysokości 1U do montażu w szafie rackowej

Stacja operatorska o parametrach nie gorszych niż:

Parametry techniczne	
Chipset	Intel B660
Płyta główna	Pro B660M-C D4CSM
TPM -	TPM 2.0
Procesor	Procesor Intel Core 13. generacji do komputerów stacjonarnych

Zgodność	Zgodność z sekcją 889 NDAA
Wyjście wideo	1x VGA/ 2x DisplayPort 1.4/ 1x HDMI 2.1
Wydajność CPU	Powyżej 30 000 pkt wg CPU Benchmark
Pamięć RAM	16 GB
System operacyjny	Microsoft Windows 11 Pro 64-bit
Dysk twardy	512 GB (w zestawie)
Pojemność zapisu danych	1 x 3.5 cala SATA Dysk twardy (opcjonalnie)
Interfejs sieci	1 x Gigabit Ethernet RJ-45 (10/100/1000 MB/s)
Parametry zasilania	
Zasilanie	100-240 VAC, 50 HZ/60 HZ 6-3 A
Pobór mocy	150 W
Moc zasilacza	300 W pojedynczy
Parametry środowiskowe	
Temperatura pracy	od +5°C do +40°C
Temperatura przechowywania	od -40°C do +65°C
Parametry fizyczne	
Wymiary	390mm x 340mm x 103mm (15.35" x 13.39" x 4.06")
Typ obudowy	Desktop / Tower

System CCTV należy zaprojektować w sposób zapewniający przechowywanie nagrań przez minimum 30 dni przy założonych parametrach nagrywania, o ile dokumentacja projektowa nie stanowi inaczej.

4. System integrujący

1. Aplikacja PSIM musi być neutralna względem integrowanych systemów.

Aplikacja PSIM musi być otwarta, tzn. poza wspieraniem funkcji integracji systemów poprzez interfejsy natywne, aplikacja PSIM musi wspierać protokoły otwarte, w tym: OPC, BACnet, KNX, Modbus RTU, Modbus IP, LON Bus.

2. Aplikacja PSIM musi być obsługiwana przez dedykowaną aplikację kliencką, wykonaną w technologii okienkowej.
Niedopuszczalne jest zastosowanie przeglądarki internetowej i technologii okien pop-up, celem eliminacji możliwości przechwycenia danych.
3. Aplikacja PSIM musi zapewniać możliwość całkowitego ukrycia systemu operacyjnego Windows przed operatorem.
4. Aplikacja PSIM musi zapewniać możliwość zdefiniowania hierarchii lokalizacji, celem uporządkowanego administrowania punktami danych oraz grupami czujników.
5. Aplikacja PSIM musi zapewniać przegląd punktów danych w dynamicznej strukturze drzewiastej, np. lokalizacja, typ systemu, grupa, czujnik.
6. Aplikacja PSIM powinna zapewniać możliwość pracy w tle, co oznacza, iż na stacji roboczej można opcjonalnie używać innych aplikacji, a w momencie wystąpienia zdarzenia/alarmu, główne okno aplikacji PSIM przesunie się na wierzch, a alarm zostanie zasygnalizowany dodatkowo akustycznie i optycznie.
7. Aplikacja PSIM musi zapewniać szyfrowanie komunikacji co najmniej na poziomie bezpieczeństwa, jaki zapewnia algorytm AES256.
8. Aplikacja PSIM musi zapewniać możliwość outsourcingu uwierzytelniania użytkowników i administrowania za pośrednictwem LDAP do Active Directory i zastosowanie profili użytkowników Active Directory.
9. Aplikacja PSIM powinna zapobiegać przedostawaniu się danych i poleceń do systemu z zewnątrz bez uzasadnienia, a także uniemożliwiać osobom trzecim dostęp do systemu. W ten sposób połączenia IP między serwerami i klientami będą szyfrowane przez TLS.
10. Aplikacja PSIM musi być dostępna w polskiej wersji językowej.
11. Aplikacja PSIM musi zapewniać możliwość obsługi zdarzeń za pomocą aplikacji mobilnej Android i iOS, z możliwością przesyłania zdjęć i automatycznego generowania zleceń.
12. Aplikacja PSIM musi oferować funkcjonalność monitorowania i wykorzystania pojemności środowiska sprzętowego aplikacji PSIM (CPU, RAM, HDD, LAN) przez sam system. W przypadku przekroczenia limitów wartości, system ma monitorować operatora o występującym problemie.
13. Aplikacja PSIM musi zapewniać pomoc kontekstową online.

14. Producent, a szczegółowo proces projektowania i produkcji oprogramowania, powinien być objęty procedurą ISO 9001:2015. Do oferty należy załączyć aktualny certyfikat.

Do oferty należy załączyć oświadczenie Producenta oprogramowania PSIM, iż aplikacja spełnia wymagania europejskiej normy DIN EN 50518 dotyczącej PSIM, w zakresie ARC (Alarm Receiving Center, w polskiej nomenklaturze Centrum Monitorowania Alarmów (CMA)).

System PSIM powinien być zaprojektowany tak, aby umożliwiał centralnie kontrolowaną interakcję między systemami bezpieczeństwa, budynku, jak i zarządzanie informacjami, jednak nie może zastępować żadnego zainstalowanego pojedynczego systemu.

Należy mieć na uwadze, iż zakres integracji zawsze zależy od możliwości zestawu SDK (Software

Development Kit) dostarczonego przez producenta integrowanego systemu i wymaga pogłębionej analizy na etapie projektowania bądź doboru poszczególnych podsystemów. Stąd wymagania przedstawione poniżej dotyczą samej funkcjonalności aplikacji PSIM.

PRAWA DOSTĘPU

1. Aplikacja PSIM musi pozwalać na definiowanie nieograniczonej liczby użytkowników, chronionych hasłem dostępu.
Użytkownik aplikacji PSIM, powinien mieć możliwość zmiany hasła po pierwszym logowaniu do systemu.
2. Aplikacja PSIM musi zapewniać możliwość zdefiniowania nieograniczonej liczby profili użytkowników. Profil określa wygląd i funkcje dostępne z poziomu interfejsu systemu oraz definiuje wszystkie prawa użytkownika.
3. Aplikacja PSIM musi umożliwiać przypisanie kilku profili jednemu użytkownikowi, między którymi może się on przełączać w dowolnym momencie.
4. Aplikacja PSIM musi zapewniać możliwość ograniczenia bądź wskazania możliwości wyboru profili, na który operator może się zalogować.
5. Prawa dostępu i edycji oraz reguły powinny być przypisane do poszczególnych profili, a następnie propagowane na użytkowników.

VIDEO

1. Aplikacja PSIM, celem prawidłowego dokumentowania zdarzeń krytycznych, musi posiadać moduł archiwum wideo, pozwalający na niezależne od systemu CCTV, gromadzenie nagrań (sekwencji) i ich wiązanie ze zdarzeniami, w ramach bazy danych systemu PSIM.
2. Aplikacja PSIM musi posiadać funkcjonalność zintegrowanego zarządzania wideo, który zapewnia dostęp do różnych systemów VMS, w tym sterowania kamerami typu PTZ oraz pełną kontrolę archiwum różnych producentów z poziomu jednorodnego i w pełni zintegrowanego GUI.
3. Aplikacja PSIM musi zapewniać wyświetlanie obrazu z dowolnych kamer (analogowe i cyfrowe), w tym samym formacie w ramach interfejsu użytkownika.
4. Aplikacja PSIM musi zapewniać wyświetlenie obrazu z kamery w ramach menadżera video (modułu CCTV), poprzez funkcję drag & drop, wybór ekranu w ramach układu i wybór kamery z grafiki (oraz na odwrót).

5. Aplikacja PSIM musi zapewniać automatyczne wyświetlenie kamery w odpowiedniego obszaru („obraz na żywo”).
6. Aplikacja PSIM musi zapewniać dostęp do archiwum i funkcji odtwarzania przy jednoczesnym wyświetlaniu obrazu na żywo.
7. Aplikacja PSIM musi zapewniać wyświetlanie wielu strumieni w ramach jednego interfejsu użytkownika, w tym w kilku definiowalnych bądź wybranych układach.
8. Aplikacja PSIM musi zapewnić nadawanie indywidualnych uprawnień dla użytkownika w zakresie obsługi wideo, jak i dostępu do kamer.
9. Aplikacja PSIM musi zapewniać funkcjonalność drag & drop dla strumieni wideo w zakresie lokalnych, jak i zdalnych ekranów wideo.
10. Aplikacja PSIM musi zapewniać zdalną kontrolę strumieni CCTV wyświetlanych w ramach ściany wizyjnej.
11. Aplikacja PSIM musi zapewniać możliwość eksportu fragmentu strumienia z kamery jako „klipu” z systemu VMS i jego zapisanie w archiwum wideo.

ZARZĄDZANIE ZDARZENIAMI

1. Aplikacja PSIM musi posiadać centralny stos alarmów, z możliwością jego dostosowywania do potrzeb użytkownika (grupowanie i sortowanie zdarzeń).
2. Aplikacja PSIM musi zapewniać możliwość konfigurowania stosu alarmu, przy czym funkcjonalność ta powinna być ograniczona prawami dostępu.
3. Aplikacja PSIM musi zapewniać akustyczną i optyczną sygnalizację przychodzących zdarzeń.
4. Aplikacja PSIM musi zapewniać filtrowanie i grupowanie zdarzeń w ramach konfigurowalnych filtrów, w ramach stosu alarmowego, jak i samodzielnej formatki systemowej.
Aplikacja PSIM musi zapewniać wyświetlenie, w zależności od typu zdarzenia, określony typ grafiki (schemat, podgląd z kamery, mapa GIS, itp.), procedurę postępowania oraz informacje powiązane, w układzie przypisanym do danego użytkownika.
5. Aplikacja PSIM musi zapewniać możliwość dodania do danego zdarzenia dokumentów powiązanych (np. pdf, jpg, docs, xlsx) poprzez funkcję drag & drop, oraz bezpośrednich komentarzy dodawanych w ramach realizacji prac przez operatorów.
6. Aplikacja PSIM musi zapewnić możliwość szybkiego wydruku – przycisk funkcyjny na oknie zdarzenia, raportu ze zdarzenia, w dowolnym momencie jego realizacji, w postaci pliku PDF, zawierającego co najmniej: unikalny numer, log wszystkich zdarzeń (działania użytkownika), grafikami zdarzenia, zrzutami ekranowymi, komentarzami, zdjęciami oraz szczegółami wiadomości.
7. Aplikacja PSIM musi zapewniać możliwość definiowania przepływów pracy (workflow) bez żadnych ograniczeń w logikę, którą można zaprogramować (skomplikowanie procedur, liczba zmiennych, złożoność procesów).
8. Aplikacja PSIM musi zapewniać możliwość informowania o wystąpieniu określonego typu zdarzenia za pomocą sms’a oraz mail’em.

9. Aplikacja PSIM musi umożliwiać przejmowanie do realizacji zdarzeń przez danego pracownika (zdjęcie ze ogólnego stosu), przypisywanie zdarzeń (ręczne, jak i automatyczne).
10. Aplikacja PSIM musi zapewniać możliwość definiowania przedziałów czasowych koniecznych na realizację poszczególnych etapów zdarzenia oraz automatyczne informowanie w przypadku braku podjęcia działań przez operatora.
11. Aplikacja PSIM, poprzez aplikację mobilną, musi zapewniać wyzwalanie nowych zdarzeń oraz śledzenie istniejących z pełną dostępnością do np. powiązanych zdjęć, nagrań głosowych, filmów.

OPERACJE KONTROLNE

- Aplikacja PSIM musi posiadać funkcjonalność planowania i automatyzacji operacji kontrolnych i serwisowych, rozumianą jako możliwość jednorazowego lub cyklicznego wprowadzenia określonego typu punktu danych (np. kamera, czytnik kontroli dostępu) w określony stan. W ramach definiowania harmonogramu, uprawniony operator, musi mieć możliwość zdefiniowania czy ów działanie podlega każdorazowej akceptacji oraz czy rozpoczęcie, jak i zakończenie podlega każdorazowemu potwierdzeniu.

GRAFIKA

1. Aplikacja PSIM musi posiadać zintegrowany graficzny interfejs użytkownika (GUI).
2. Aplikacja PSIM musi zapewniać modułową strukturę graficzną, tj, każda grafika może zostać wstawiona jako moduł do innej grafiki.
3. Aplikacja PSIM musi zapewniać możliwość wyświetlania wielu treści jednocześnie tj. map, grafik, przycisków, paska narzędziowego, strony internetowej, kanałów RSS, stosu zdarzeń i alarmów, etc.
4. GUI aplikacji PSIM musi zapewniać możliwość interakcji ze ścianami wizyjnymi w wykorzystaniem metody drag & drop.
5. GUI aplikacji PSIM nie może ograniczać liczby wyświetlanych jednocześnie okien.
6. GUI aplikacji PSIM nie może ograniczać liczby definiowanych widoków.
Aplikacja PSIM musi zapewniać bezpośredniego osadzania grafiki, w standardowych formatach (.wmf, .emf, .sld, .bmp, .jpg, .png, .tif, .gif,) oraz formatach CAD (AutoCAD. dxf i .dwg oraz Microstation. dgn), w grafice aplikacji PSIM.
7. Aplikacja PSIM musi zapewniać automatyczną aktywację symboli czujników i zmiany w grafikach wprowadzanych w połączonych z aplikacją plikami w formacie CAD.
8. Aplikacja PSIM, poprzez edytor graficzny musi umożliwiać tworzenie własnych symboli oraz edytowanie już istniejących.
9. Aplikacja PSIM powinna zapewniać podstawową bibliotekę symboli do różnych przypadków użycia.
10. Aplikacja PSIM musi zapewniać możliwość wstawiania do grafik oraz tekstu przycisków z przypisanymi akcjami.

11. Aplikacja PSIM musi zapewniać możliwość definiowania warstw, czyli pozwalać na logiczne grupowanie określonych typów informacji (np. typów punktów danych) i ich wyświetlanie bądź ukrywanie w zależności od przypadku użycia.

ARCHIWIZACJA

1. Aplikacja PSIM musi zapewniać pełną archiwizację przetwarzanych zdarzeń.
2. Aplikacja PSIM musi zapewniać możliwość filtrowania archiwum za pomocą zmiennych filtrów.
3. Aplikacja PSIM musi zapewniać wyświetlenie zarchiwizowanego zdarzenia ze wszystkimi powiązanymi informacjami (takimi samymi jak podczas przetwarzania zdarzenia).
4. Aplikacja PSIM musi zapewniać logowanie wszystkich działań podejmowanych przez operatora.
5. Aplikacja PSIM musi zapewniać możliwość dostępu do poszczególnych lokalizacji, jak i punktów danych.

System PSIM powinien umożliwiać budowę architektury wysokiej dostępności (HA) obejmującej redundancję serwerów aplikacyjnych oraz baz danych, bez utraty funkcjonalności systemu.

5. Wymagania ogólne dla systemów bezpieczeństwa

Integracja z systemami istniejącymi u Zamawiającego

Wszystkie systemy bezpieczeństwa budynkowego przewidziane do realizacji w ramach niniejszego zamówienia (w szczególności system kontroli dostępu, telewizji dozorowej, sygnalizacji włamania i napadu oraz platforma integrująca) muszą zapewniać pełną integrację funkcjonalną z systemami aktualnie eksploatowanymi przez Zamawiającego. Nadrzędną zasadą doboru rozwiązań jest rozbudowa istniejącego środowiska bezpieczeństwa, a nie tworzenie środowiska równoległego — nowe instalacje muszą stanowić z systemami istniejącymi jedno-litą całość funkcjonalną, zarządzaną z poziomu wspólnego interfejsu operatorskiego.

W szczególności oznacza to, że:

1. Wykonawca zobowiązany jest na etapie projektowania zinwentaryzować systemy bezpieczeństwa eksploatowane przez Zamawiającego oraz uzgodnić z Zamawiającym sposób integracji nowych instalacji z tymi systemami, a przyjęte rozwiązania przedstawić Zamawiającemu do akceptacji przed przystąpieniem do realizacji.
2. Dostarczone urządzenia i oprogramowanie muszą być zgodne z platformami zarządzającymi użytkowanymi przez Zamawiającego lub zapewniać komunikację z nimi w oparciu o otwarte, udokumentowane standardy i protokoły komunikacyjne (m.in. interfejsy API producenta, standardy branżowe stosowane w systemach zabezpieczeń), bez

konieczności ponoszenia przez Zamawiającego dodatkowych kosztów licencyjnych nieuwjętych w ofercie.

3. Niedopuszczalne jest zastosowanie rozwiązań zamkniętych, uniemożliwiających rozbudowę systemu lub jego serwisowanie przez podmioty inne niż dostawca, ani rozwiązań wymagających wymiany infrastruktury już posiadanej przez Zamawiającego, o ile infrastruktura ta spełnia wymagania techniczne dla planowanych funkcji.

4. Elementy identyfikacji użytkowników (w tym nośniki i format danych kontroli dostępu) muszą być zgodne z systemem identyfikacji stosowanym przez Zamawiającego, tak aby użytkownicy mogli korzystać z dotychczasowych identyfikatorów bez ich wymiany.

5. Odpowiedzialność za skuteczność integracji, w tym za uzyskanie niezbędnych licencji, sterowników i wsparcia producentów systemów istniejących, spoczywa w całości na Wykonawcy.

Cyberbezpieczeństwo

Wszystkie urządzenia oraz oprogramowanie wchodzące w skład systemów KD, CCTV, SSWiN oraz PSIM muszą spełniać poniższe wymagania:

1. komunikacja administracyjna realizowana wyłącznie z wykorzystaniem protokołów szyfrowanych (HTTPS, TLS 1.2 lub nowszy),
2. wymagana możliwość zmiany haseł domyślnych oraz ich wymuszonej zmiany przy pierwszym logowaniu,
3. możliwość tworzenia indywidualnych kont użytkowników z nadawaniem uprawnień zgodnie z rolami,
4. wszystkie operacje administracyjne muszą być rejestrowane w dziennikach zdarzeń systemu,
5. urządzenia muszą umożliwiać synchronizację czasu z serwerem NTP,
6. oprogramowanie systemowe i firmware urządzeń powinny posiadać możliwość aktualizacji bez konieczności wymiany urządzeń,
7. niedopuszczalne jest pozostawienie aktywnych niewykorzystywanych usług sieciowych,
8. Wszystkie urządzenia sieciowe, serwery i systemy bezpieczeństwa powinny umożliwiać monitoring przy wykorzystaniu protokołu SNMPv3,
9. Wszystkie systemy KD, CCTV, SSWiN oraz PSIM muszą korzystać ze wspólnego źródła czasu NTP wskazanego przez Zamawiającego.

Ogólne wytyczne dla SKD oraz CCTV

1. Kontrolery kontroli dostępu muszą znajdować się w pomieszczeniach objętych kontrolą dostępu.
2. Węzły sieciowe oraz inne wybrane na etapie projektu pomieszczenia muszą być objęte dwustronną kontrolą dostępu

3. W przypadku braku możliwości objęcia kontrolą dostępu pomieszczenia w której znajduje się szafa teletechniczna, szafę taką należy zabezpieczyć kontrolą dostępu w postaci czytnika montowanego na jej froncie oraz rygla elektromagnetycznego.
4. Wejścia do pomieszczeń objętych kontrolą dostępu muszą być w polu widzenia kamer, szafy w pomieszczeniach teletechnicznych muszą być w polu widzenia kamer.
5. Wszystkie wejścia do budynku muszą być objęte kontrolą dostępu.

Dokumentacja powykonawcza

W ramach odbioru końcowego Wykonawca zobowiązany jest przekazać Zamawiającemu kompletną dokumentację powykonawczą w wersji papierowej oraz elektronicznej.

Dokumentacja powinna zawierać co najmniej:

1. schematy ideowe i wykonawcze instalacji w formacie PDF i DWG,
2. rzuty obiektu z naniesioną lokalizacją wszystkich urządzeń,
3. bilans mocy wszystkich zasilaczy i obwodów zasilających,
4. wykaz zastosowanych urządzeń wraz z numerami seryjnymi,
5. adresację IP wszystkich urządzeń sieciowych,
6. konfiguracje systemów KD, CCTV, SSWiN i PSIM w postaci kopii bezpieczeństwa umożliwiającej pełne odtworzenie systemu,
7. instrukcję eksploatacji i procedury awaryjne,
8. wyniki wszystkich testów odbiorczych,
9. wykaz kont administracyjnych przekazywanych Zamawiającemu.

Testy odbiorcze

Przed podpisaniem protokołu odbioru należy przeprowadzić testy funkcjonalne wszystkich systemów.

Zakres testów powinien obejmować co najmniej:

Kontrola dostępu

1. poprawność odczytu kart,
2. działanie harmonogramów dostępu,
3. poprawność działania kontaktronów,
4. działanie przycisków wyjścia,
5. działanie przejść podczas zaniku zasilania,
6. współpracę z systemem SSP.

CCTV

1. poprawność rejestracji obrazu,
2. odtwarzanie nagrań archiwalnych,
3. działanie wszystkich wymaganych analiz obrazu,
4. poprawność eksportu materiału dowodowego,

5. działanie integracji z PSIM.

SSWiN

1. wykrywanie naruszeń przez wszystkie czujki,
2. wykrywanie sabotażu urządzeń,
3. poprawność uzbrajania i rozbrajania stref,
4. działanie wszystkich sygnalizatorów.

PSIM

1. poprawność odbioru zdarzeń ze wszystkich systemów,
2. działanie scenariuszy alarmowych,
3. poprawność wizualizacji zdarzeń,
4. generowanie raportów i archiwizacja zdarzeń.

Wymagania dotyczące infrastruktury szaf teletechnicznych

Szafy teletechniczne przeznaczone dla systemów bezpieczeństwa powinny spełniać następujące wymagania:

1. uporządkowane prowadzenie przewodów z wykorzystaniem organizatorów kabli,
2. trwałe oznaczenie wszystkich urządzeń, przewodów i portów,
3. możliwość zamknięcia na zamek mechaniczny lub objęcia kontrolą dostępu,
4. zapewnienie odpowiedniej wentylacji urządzeń.

Okablowanie

Dla wszystkich systemów bezpieczeństwa należy stosować następujące zasady wykonawcze:

1. pozostawienie minimum 0,5 m zapasu przewodu przy urządzeniach końcowych,
2. pozostawienie minimum 2 m zapasu przewodu w szafach teletechnicznych,
3. zachowanie separacji przewodów niskoprądowych od instalacji 230V zgodnie z obowiązującymi normami i wytycznymi producentów,
4. wszystkie przewody muszą zostać oznakowane trwałymi identyfikatorami.

