**Załącznik B8E - Wytyczne w zakresie rozbudowy SZB**

Obiekt Elektrociepłowni Gryfino zaliczany jest do Infrastruktury Krytycznej. Jest elementem strategicznym dla zapewnienia dostaw energii cieplnej dla mieszkańców Gryfina i okolic. Teren ochrony jest terenem rozległym, o mocnym zadrzewieniu, z dala od skupisk ludzkich. Przedmiotem zadania jest wykonanie prac polegających na zabezpieczeniu nowej infrastruktury w celu zapewnienia ochrony zgodnie z aktualnymi wymaganiami formalno-prawnymi, przy zachowaniu unifikacji sprzętowo-programowej z funkcjonującymi już na terenie PGE EC Szczecin oraz EC Pomorzany systemami bezpieczeństwa (ochrona obwodowa, VSS, SSWiN, SKD, SSP, PSIM). Systemy te należy rozbudować o obszar ogrodzenia oraz poszczególnych obiektów, a następnie zintegrować w ramach systemu zarządzania bezpieczeństwem i wizualizacji PSIM. Systemy mają mieć funkcjonalność zarządzania i wymiany informacji oraz nadawania uprawnień i zmian konfiguracji z poziomu istniejących jednostek operatorskich istniejących w EC Szczecin i EC Pomorzany. Dlatego też należy zapewnić pełną integralność i spójność na poziomie sprzętowym i programowym z istniejącymi w PGE EC Szczecin oraz EC Pomorzany systemami bezpieczeństwa tzn. system monitoringu wizyjnego VSS, system kontroli dostępu KD, system sygnalizacji włamania i napadu SSWiN, instalacja okablowania strukturalnego TECH-LAN, system sygnalizacji pożaru SSP, system wizualizacji i zarządzania bezpieczeństwem SZB - PSIM. Prowadzone prace nie mogą zakłócić ciągłości pracy poszczególnych instalacji bezpieczeństwa. Wszelkie roboty należy prowadzić w porozumieniu z Zamawiającym i konserwatorem systemu w taki sposób, aby nie naruszyć warunków gwarancji.

Wszystkie prace przewidziane do realizacji w obszarze nowych lokalizacji oraz modyfikacji i rozbudowy istniejących systemów bezpieczeństwa, wykorzystanie szaf dystrybucyjnych, przełącznic światłowodowych, obwodów zasilania i innych niezbędnych do realizacji zadania należy wykonać w uzgodnieniu i po uzyskaniu pisemnej zgody Zamawiającego. Wprowadzone zmiany i prace modernizacyjne nie mogą naruszyć integralności, spójności i ciągłości pracy i ochrony gwarancyjnej istniejącego systemu bezpieczeństwa.

Prace montażowe oraz konfiguracyjne mogą być wykonywane jedynie przez osoby posiadające aktualne szkolenie z zakresu konfiguracji, programowania i serwisowania systemów bezpieczeństwa oraz wizualizacji i zarzadzania bezpieczeństwem funkcjonujących w ramach struktury zabezpieczeń PGE EC Szczecin oraz EC Pomorzany, wydane przez producenta lub dystrybutora danego systemu.

**System ochrony obwodowej**

Teren nadzorowany elektronicznymi systemami bezpieczeństwa powinien być ogrodzony ogrodzeniem panelowym, przenoszącym drgania mechaniczne, powstałe w przypadkach wdrapywania się na ogrodzenia, przecinanie ogrodzenia, demontażu ogrodzenia. Zalecana wysokość ogrodzenia to 250cm, rozmiar oczka – na tyle wąski, by uniemożliwić wsunięcie w nie rąk i stóp dorosłej osoby, słupek panelowy z profili zamkniętych i zakończony rozgałęzieniem typu Y, panel zakończony zasiekiem spiralnym z drutu ostrzowego, nierdzewnego, kręgi umieszczone prostopadle do osi ogrodzenia, zamocowane na trzech rzędach prostego drutu ostrzowego. Zasiek spiralny o średnicy kręgu 450mm o gęstości 6 zwojów na metr. Panele ogrodzenia powinny łączyć się ze sobą za pomocą elementów spinających przenoszących drgania i montowane do słupów od czoła słupa. Panel posadowiony na podmurówce prefabrykowanej żelbetowej, L=2,48, h=0,5m, e=0,057m. Do montażu paneli, podwalin, zasieków i drutu nośnego należy używać wyłącznie elementów systemowych. Ogrodzenie powinno zostać zabezpieczone antykorozyjnie za pomocą ocynku i powłoki poliestrowej.

Obiekty zespołu kotłów gazowych należy zabezpieczyć elektronicznymi systemami zabezpieczeń, które należy wykonać jako rozszerzenie i rozbudowę istniejących systemów zainstalowanych i funkcjonujących w tym obszarze o nowe elementy.

Systemy i instalacje przewidziane do rozbudowy:

* System ochrony obwodowej w oparciu o system ochrony napłotowej oraz czujki dopplerowskie, w miejscach braku ciągłości linii ogrodzenia, np. bramy przesuwne, podejście od strony wody;
* System monitoringu wizyjnego VSS;
* System kontroli dostępu SKD;
* System sygnalizacji włamania i napadu SSWiN;
* Wydzielona sieć teleinformatyczna na potrzeby systemów bezpieczeństwa Tech-LAN;
* System monitorowania parametrów środowiskowych punktów dystrybucyjnych PPD;
* System wizualizacji i zarządzania bezpieczeństwem SZB – PSIM (Physical Security Informaction Management).

Należy wykonać system ochrony obwodowej w oparciu o system ochrony napłotowej oraz czujki dopplerowskie. System ochrony obwodowej należy wykonać jako rozbudowę istniejącego w obszarze ogrodzenia terenu EC Pomorzany systemu przy zachowaniu pełnej integracji z istniejącymi systemami: zarządzania bezpieczeństwem PSIM, kontroli dostępu SKD, systemu sygnalizacji włamania i napadu SSWiN oraz monitoringu wizyjnego VSS przy użyciu dedykowanych interfejsów sprzętowo-programowych oraz wzajemnych zasterowań. W tym celu należy istniejący system rozbudować o dedykowane kontrolery w lokalizacji EC Gryfino (kompatybilne z istniejącym systemem), detektory, czujki oraz oprogramowanie niezbędne do zabezpieczenia nowych lokalizacji. Nowe elementy zwizualizować w systemie PSIM.

System ochrony napłotowej powinien składać się z sensorów z trójosiowymi sensorami MEMS (sensory mikro elektro-mechaniczne), pogrupowanymi po siedem sensorów. Grupy powinny składać się minimum z jednego sensora głównego i sześciu pomocniczych. System powinien umożliwić instalacje min. 20 czujników głównych oraz min. 120 czujników pomocniczych rozstawionych do 5m od siebie, w ramach jednego kontrolera. Każdy z sensorów pomocniczych powinien działać indywidualnie i generować własny sygnał wysyłany niezależnie do sensora głównego, który przekazuje je do kontrolera. Kontroler systemu powinien zbierać informacje na temat stanu sensorów głównych i pomocniczych, dzięki czemu możliwe powinno być analizowanie docierających z nich informacji w odniesieniu do innych sensorów. Kontroler dzięki aproksymacji powinien wykrywać i rejestrować miejsce zdarzenia z dokładnością do jednego metra. Wszystkie grupy powinny łączyć się z kontrolerem za pomocą dwóch niezależnych magistral. Czujniki na obu magistralach, niezależnie od przynależności do grupy czy magistrali powinny umożliwiać podział logiczny na min. 80 dowolnej długości stref w obrębie jednego kontrolera. Dzięki możliwości analizowania parametrów pojedynczego sensora, system powinien być adaptowany do różnych rodzajów ogrodzenia nawet, jeżeli występują one w obrębie jednego kontrolera. Możliwe powinno być jest dopasowanie parametrów pracy indywidualnie dla każdej strefy, a także dla każdego sensora. Wysokie prawdopodobieństwo wykrycia oraz niski poziom fałszywych alarmów powinien być wynikiem precyzyjnego pomiaru, przez każdy sensor drgań występujących w trzech płaszczyznach i ich analizy przez sterownik. Analiza powinna odbywać się przy zastosowaniu algorytmu logiki rozmytej (fuzzy logic).

System odbierając sygnały generowane przez ogrodzenie powinien potrafić rozróżnić próbę włamania od uszkodzenia lub wspinania się na ogrodzenie, co powinno pozwolić na eliminowanie fałszywych alarmów. Czujniki rozmieszczone na ogrodzeniu powinny wykrywać wibracje spowodowane przez próbę włamania i konwertować je na postać cyfrową, które powinny być następnie analizowane wstępnie przez czujnik główny dla danej grupy czujników. Informacje powinny być następnie wysyłane za pośrednictwem magistrali szeregowej RS485 do kontrolera, który między innymi powinien przechowywać wszystkie dane związane z włamaniami z odpowiadającą im datą i godziną. System powinien być wtedy w stanie przesłać dane alarmowe w czasie rzeczywistym do innych systemów kontroli, aby np. aktywować przekaźniki do sygnalizacji alarmowej lub też umożliwić podgląd naruszanego odcinka ogrodzenia za pomocą systemu monitoringu wizyjnego.

Cechy systemu ochrony napłotowej:

* Wykrywanie przecięć, wspinania się na ogrodzenie, podnoszenie lub przemieszczanie segmentu ogrodzenia,
* Wykorzystanie technologii MEMS,
* Analiza sygnału przy pomocy algorytmu logiki rozmytej,
* Możliwość instalacji systemu na różnego typu ogrodzeniach w obrębie jednego kontrolera,
* Natywny adres IP,
* Redundancja przesyłu informacji do kontrolera w wyniku przerwania linii magistrali,
* Detekcja położenia sensora precyzyjna lokalizacja intruza ,
* Temperatura pracy min. z zakresu od -40 do 70°C, wilgotność min. z zakresu od 0-100%.

Elementy systemu ochrony obwodowej należy zwizualizować na planach w systemie nadrzędnym PSIM – wykorzystując oprogramowanie zarządzające ochroną napłotową oraz dedykowane interfejsy programowo-sprzętowe systemu PSIM. Integrację systemu ochrony napłotowej z SSWIN należy wykonać przy użyciu wzajemnych zasterowań, z uwzględnieniem nadzoru min. alarmu z grupy systemu napłotowego oraz brak 230VAC, awaria akumulatora, sabotaż układu zasilania systemu napłotowego.

W miejscach fizycznego braku ciągłości ogrodzenia należy zastosować czujki dopplerowskie, tj. czujki mikrofalowe (czujki monostatyczne) przeznaczone do ochrony zewnętrznej o poniższych minimalnych wymaganiach funkcjonalno-użytkowych:

* Zasięg min. 12 lub 24m w zależności od konfiguracji
* Wykorzystanie efektu Dopplera z modulacją dwóch częstotliwości
* Min. 4 kanały modulacji
* Zapas mocy dla kompensacji warunków propagacji min. ≥16 dB
* Cyfrowa analiza sygnału przy użyciu algorytmu “FUZZY LOGIC”
* Dynamiczny cyfrowy antymasking
* Liniowa polaryzacja wiązki mikrofalowej
* Funkcja SRTD (Short Range Target Discrimination) tj. odróżnienie ruchu blisko czujnika spowodowany przez małe zwierzęta, ptaki
* Funkcja LRTD (Long Range Target Discrimination) tj. niewrażliwość na zbyt odległe obiekty
* Prędkość wykrywania obiektu min. z zakresu od 30 mm/2 do 15 m/s
* Możliwość komunikacji przez sieć IP i zasilania w technologii PoE
* Dedykowane oprogramowanie do regulacji i serwisowania urządzeń
* Obudowa wykonana z poliwęglanu o wysokiej wytrzymałości.

Czujki dopplerowskie systemu ochrony obwodowej należy zwizualizować na planach zagospodarowania terenu w systemie nadrzędnym PSIM – wykorzystując oprogramowanie zarządzające ochroną napłotową oraz dedykowane interfejsy programowo-sprzętowe systemu PSIM oraz wzajemne zasterowania z systemem SSWIN, min. alarm, sabotaż, awaria czujki dopplerowskiej.

**System monitoringu wizyjnego VSS**

Obszar ogrodzenia, portierni, ciągi komunikacyjne, wejścia do newralgicznych stref i obiektów należy objąć systemem monitoringu wizyjnego opartym o szybkoobrotowe kamery IP o parametrach zgodnych z poniższymi wymaganiami funkcjonalno-użytkowymi. Kamery te powinny nadzorować obszary przypisane do stref systemu napłotowego w min. rozdzielczości 250px/m tj. w funkcji identyfikacji wg PN-EN 62676-4 z chwilą wystąpienia zdarzenia alarmowego, a poza tym trybem w funkcji min. rozpoznania tj. 125px/m. W pozostałych obszarach, takich jak bramy wjazdowe, furtki, przejścia objęte kontrolą dostępu należy zapewnić nadzór w rozdzielczości 250px/m przy użyciu kamer stałopozycyjnych.

Na potrzeby nowych punktów obsługi (np. nastawnie, pomieszczenia ruchu) system VSS wyposażyć w nowe jednostki dostępowe dla operatorów systemu VSS.

System monitoringu wizyjnego VSS należy wykonać jako rozbudowę istniejącego systemu VSS przy zachowaniu pełnej integracji z istniejącymi systemami: zarządzania bezpieczeństwem PSIM, kontroli dostępu SKD oraz systemu sygnalizacji włamania i napadu oraz ochrony obwodowej SSWiN przy użyciu dedykowanych interfejsów sprzętowo-programowych oraz wzajemnych zasterowań.

Najważniejsze urządzenia zarządzające systemem telewizji dozorowej (rejestratory lub grupy rejestratorów, oprogramowanie zarządzające i integrujące rejestratory, stacje podglądowe, macierze dyskowe) powinny spełniać następujące wymagania techniczno- użytkowe:

* Użyty sprzęt i materiały powinny być komponentami standardowymi dostępnymi w stałej ofercie danego producenta.
* Wszystkie systemy powinny być przetestowane i wdrożone w istniejących instalacjach.
* Gwarancja producenta nie powinna być krótsza niż 24 miesiące od daty dostawy.
* Producent urządzenia lub jego reprezentant powinien udostępniać linię telefoniczną dla wsparcia technicznego, dostępną przez wszystkie dni robocze w godzinach pracy tych firm.
* Producent zagwarantować powinien minimum 8 lat wsparcia serwisowego urządzeń od momentu ich zakupu uwzględniając dostawę części zamiennych lub wymianę z zachowaniem funkcjonalności
* System powinien pozwalać na rozszerzenie funkcjonalności poprzez uaktualnienie oprogramowania bez potrzeby zmian w strukturze sprzętowej.
* Pojedyncze urządzenie służące do zapisu obrazów ze wszystkich podłączonych do niego kamer, umożliwiać powinno zainstalowanie wewnątrz urządzenia dysków twardych o pojemności minimum 96 TB umieszczonych w kieszeniach „hot swap”, z możliwością konfiguracji przestrzeni dyskowej przynajmniej w formie RAID 5 lub RAID 6 oraz dodatkowo możliwość podłączenia zewnętrznych macierzy dyskowych rozszerzających obsługiwaną pojemność dyskową do 256 TB
* Każde urządzenie powinno umożliwiać zapis i zarządzenie w tym płynne zarządzanie wszystkimi urządzeniami na obiekcie z zachowaniem możliwości rozbudowy na poziomie 30%
* System (w podanej konfiguracji lub po odpowiedniej rozbudowie) powinien umożliwiać jednoczesne podłączenie kamer analogowych i sieciowych lub serwerów sieciowych rożnych producentów, aby zapewnić możliwość wyboru odpowiedniego rodzaju kamery i uniezależnić się od jednego dostawcy kamer.
* Zamawiający wymaga aby zaimplementowane były minimum: 10 protokołów do sterowania kamerami obrotowymi, 300 typów kamer IP lub serwerów sieciowych, 100 typów kamer MPixelowych, a także powinny być wspierane (dla podglądu i zapisu) standardy ONVIF i RTSP
* Do zapisu obrazu z kamer wykorzystany powinien być cyfrowy rejestrator sieciowy. Powinien on umożliwiać wykorzystanie zaawansowanej technologicznie kompresji typu MPEG4 i/lub H.265 zoptymalizowanej i zaadoptowanej do wykorzystania w profesjonalnych systemach nadzoru VSS, dostępnej dla każdego obsługiwanego kanału oraz JPEG – użytkownik powinien mieć możliwość wyboru rodzaju kompresji w zależności od zastosowanych kamer, ich funkcji w systemie itp.
* System powinien umożliwiać transkodowanie „w locie” sygnałów z kamer IP do kodeka zoptymalizowanego dla VSS
* Algorytm kompresji i dekompresji (w przypadku H.265 powinien umożliwiać niezależne definiowanie parametrów pracy dla każdego kanału (wejścia) wideo, z uwzględnieniem ustawienia długości struktury GOP lub częstości występowania klatek bazowych; zagwarantuje to dopasowanie do charakterystyki obserwowanej sceny i umożliwi dokładne definiowanie parametrów przepływności strumienia danych.
* System powinien być przygotowany do rejestracji/zarządzania przy użyciu kodeka H.265.
* System powinien obsługiwać połączenie sieciowe z obsługą protokołu TCP/IP i prędkością połączenia 1 GBit/sekundę. W przypadku wykorzystywania kamer sieciowych, każdy z serwerów rejestrujących posiadać powinien minimum podwójną kartę Ethernetową (pierwsza dla sygnałów przychodzących z kamer, druga dla strumieni wysyłanych do stacji podglądowych). Przy zastosowaniu macierzy iSCSI rejestrator powinien być wyposażony w nadmiarowe karty sieciowe.
* Urządzenie powinno być wyposażone w redundantny zasilacz. Jest to niezbędne. Jakakolwiek awaria zasilacza podstawowego powinna być zgłaszana i zasilacz rezerwowy powinien być przełączony automatycznie w trybie natychmiastowym. Wymiana zasilaczy powinna być możliwa bez konieczności wyłączania NVR/DVR (Hot Swap).
* Urządzenie musi być podłączone do dwóch niezależnych torów zasilania z czego przynajmniej jeden musi być podłączony do instalacji zasilania gwarantowanego.
* System powinien umożliwiać lokalny podgląd na żywo, odtwarzanie i nagrywanie wszystkich podłączonych kamer. Funkcja podglądu bez ograniczeń musi być dostępna również poprzez połączenie sieciowe z rejestratorem.
* Dla wybranych użytkowników istnieć musi możliwość zdefiniowania niezależnych ograniczeń co do podglądu na żywo i/lub odtwarzania kamer.
* Prędkość przetwarzania obrazów z podłączonych kamer sieciowych powinna być zależna wyłącznie od możliwości i parametrów samej kamery i nie powinna być w żaden sposób ograniczona przez rejestrator.
* System powinien być skalowany i rozszerzalny aby umożliwić prostą rozbudowę w razie takiej potrzeby.
* Prędkość rejestracji, rozdzielczość i jakość powinna być ustalana przez użytkownika niezależnie od parametrów strumieni do podglądu "na żywo". Konfiguracja powinna umożliwiać zmianę parametrów rejestracji „w locie” (bez konieczności zmiany parametrów kamery/kodera z aplikacji konfiguracyjnej – wcześniej predefiniowane parametry dla rejestracji) dla każdej kamery niezależnie, w różnych trybach pracy: nagrywanie ciągłe, nagrywanie zgodnie z harmonogramem czasowym oraz nagrywanie pre-alarmowe i alarmowe konfigurowane indywidualnie dla różnych typów zdarzeń alarmowych
* Dostępna przestrzeń dyskowa zespołu rejestratorów powinna być zorganizowana logicznie w formie odrębnych segmentów (pierścieni, z ang. ring). Pozwoli to na prowadzanie zapisu z różnymi parametrami odnośnie czasu i priorytetu przechowywania zapisu z poszczególnych kamer i zdarzeń. System powinien udostępniać co najmniej 5 pierścieni zapisu i 3 poziomów (priorytetów) zapisu. Zapis na pierścieniach powinien odbywać się poprzez automatyczne nadpisywanie i zastępowanie najstarszych nagrań.
* Wielkość poszczególnych „ringów” jaki i całej bazy danych dobierana, zmieniana i aktualizowana powinna być dynamicznie przez system, zapewniając optymalne wykorzystanie przestrzeni dyskowej i uzyskanie maksymalnych czasów archiwizacji.
* Nie dopuszcza zastosowania systemów, w których przestrzeń dyskową dla poszczególnych kamery ustawia się w sposób stały i niezmienny w procesie konfiguracji, przyporządkowując danej kamerze fragment dostępnej przestrzeni dyskowej
* System wyposażony powinien być w bazę danych dla multimediów oraz dodatkową w pełni zsynchronizowaną bazę danych dla zdarzeń, w formacie standardowej i udokumentowanej bazy SQL (możliwość prostej wymiany danych z aplikacjami zewnętrznymi
* Dla wydłużenia czasu archiwizacji materiału video, system powinien umożliwiać zmianę ilości klatek już zarejestrowanego materiału – rozrzedzanie zapisu. Oznacza to, że po wcześnie zaprogramowanym przez użytkownika czasie, system automatycznie usunie zdefiniowaną przez użytkownika część zarejestrowanego materiału.
* Przykładowo: przy normalnej rejestracji prędkość zapisu wynosiła 25kl/sek. Po tygodniu należy zachować tylko 5 klatek/s (spośród zapisanych wcześniej w ciągu każdej sekundy 25 klatek należy odpowiednio wykasować 20 klatek zarejestrowanego materiału).
* System powinien obsługiwać dynamiczną transmisję strumieniową, w celu optymalizacji obciążenia sieci, obniżenia wymagań dla dekompresji obrazu i zwiększenia wydajności wyświetlania na stacjach podglądowych. W tym celu rozdzielczość transmitowanych "na żywo" obrazów powinna automatycznie dostosowywać się do rozmiaru (rozdzielczości) okien podglądu, w których wyświetlane są obrazy z poszczególnych kamer na stacji podglądowej. Dopasowanie to zależne powinno być od typu zastosowanej kamery, jednak system przy współpracy z wybranymi kamerami umożliwiać powinien automatyczne dopasowanie minimum do rozdzielczości: QCIF, QVGA, VGA, SVGA, WXGA, 720p, 1080p, 3MPix, 5MPix, 8MPix, 12MPix
* System powinien umożliwiać generowanie zdarzeń oraz tworzenie harmonogramów czasowych w oparciu o zegar astronomiczny zaprogramowany na postawie lokalizacji geograficznej (dynamiczne obliczanie wschodów i zachodów słońca)
* Zarządzanie zdarzeniami i alarmami powinno pozwalać na efektywną adaptację reakcji systemu na stany alarmowe oraz inne zdarzenia, zgodnie z wymaganiami użytkownika. Reakcje systemu powinny uwzględniać:
  + Zdefiniowane przez użytkownika dowolnego czasu trwania sekwencji wideo przed i po wystąpieniu alarmu;
  + Parametry rejestracji (jakość i prędkość) niezależne (indywidualne) dla wszystkich kamer;
  + Automatyczne wyświetlanie obrazów alarmowych zdefiniowanych przez użytkownika (na żywo i/lub stop klatki alarmowej ) na predefiniowanych stacjach roboczych;
  + Zmiana stanu jednego lub kilku styków wyjściowych przekaźników;
  + Wysyłanie informacji o alarmach lub zdarzeniach do zalogowanych użytkowników,
  + Obsługa interfejsów do systemów innych producentów;
  + Ustawienie jednej lub wielu kamery PTZ w zaprogramowanej pozycji;
  + Rozpoczęcie tworzenia automatycznych kopii zapasowych przedefiniowanych sekwencji w razie wystąpienia alarmu, bądź innego zdarzenia;
  + Wysyłanie komunikatów email do zdefiniowanych adresatów, również z załączonymi obrazami alarmowymi
* Generowanie alarmów powinno następować co najmniej na skutek następujących zdarzeń: wewnętrzna analiza obrazu, zewnętrzne wejścia alarmowe oraz interfejsy z systemów innych producentów (szeregowe lub łącze TCP/IP).
* System udostępniać powinien harmonogramy czasowe do kontroli przetwarzanych zdarzeń oraz parametrów rejestracji. Pozwala to na całkowicie bezobsługowe działanie systemu, np. włączenie funkcji detekcji (wykrywania) ruchu w określonym przedziale czasowym, lub sprawdzanie stanu styków wejściowych w określonych przedziałach czasowych. System udostępnia co najmniej 80 definiowanych przez użytkownika przedziałów czasowych.
* System udostępniać powinien funkcję „inteligentnego podglądu sceny”. W tym trybie wybór danej kamery powinien automatycznie wyświetlić scenę złożoną z tej kamery i kamer z jej otoczenia dając pełen przegląd sytuacji na monitorowanej scenie.
* W celu odnalezienia określonego nagrania wideo, operator nie musi wybierać odpowiedniego urządzenia nagrywającego. Użytkownikowi powinna być udostępniona jednolita lista wszystkich dostępnych kamer, niezależnie od tego, do jakiego rejestratora DVR/NVR kamery te są podłączone.
* System powinien posiadać opcję szyfrowania zgrywanego na nośniki zewnętrzne materiału,
* W trakcie procesu eksportowania lub tworzenia kopii zapasowych, oprogramowanie odczytujące kopię nagrań powinno zostać automatycznie umieszczone razem z sekwencjami wideo na nośniku magazynującym, aby umożliwić przegląd wyeksportowanych obrazów na standardowym komputerze klasy PC z systemem Windows11 w wersji Professional 64 bitowej lub nowszym, dzięki czemu można uniknąć naruszenia ich integralności oraz unika się potrzeby dodatkowego instalowania oprogramowania przeglądającego.
* Możliwe powinno być automatyczne tworzenie kopi zapasowych całości lub wybranej części materiału. System powinien zarządzać zapisanymi kopiami nagrań udostępniając co najmniej opcje: dzielenie dużych plików na części przy ich tworzeniu, szyfrowanie tworzonych plików (hasło), limitowanie pasma zajmowanego przez proces backupu, autousuwanie najstarszych nagrań po zdefiniowanym czasie lub przekroczeniu wielkości zdefiniowanej przestrzeni dyskowej.
* System umożliwiać powinien tworzenie kopii fragmentów lub całości zarejestrowanego materiału. Konfiguracja tworzenie kopii zapasowych powinna pozwolić użytkownikowi wskazywać różne katalogi dla przechowywania kopii zapasowych na nośnikach magazynujących połączonych lokalnie lub poprzez sieć, dla różnych zdarzeń dotyczących tworzenia kopii zapasowych.
* Tworzenie kopii zapasowych powinno być możliwe regularnie, we wcześniej określonych godzinach lub dniach jak również wywoływać je powinien dowolny alarm lub zdarzenie systemowe.
* Powinna istnieć możliwość rozróżniania między kopiami zapasowymi nagrań ciągłych oraz alarmów lub zdarzeń, przy dodatkowym rozróżnianiu poziomu alarmu lub zdarzenia.
* Zbiór parametrów opisujących tworzenie kopii zapasowej zależnie od przyczyn wywołujących tą kopię (opisanych w punkcie powyżej) umożliwia co najmniej zdefiniowanie docelowego katalogu, czasu archiwizacji oraz zachowania związanego z nadpisywaniem starych plików kopii zapasowych.
* Urządzenie/system VSS powinien mieć możliwość komunikacji z systemami firm trzecich takich jak kontrola dostępu, Zarządzania Budynkami, Zarządzania łańcuchem dostaw i innymi
* Powinna istnieć możliwość połączenia każdej metadanej zdarzenia z zapisanym obrazem pozwalająca na używanie tych danych jako kryterium dla dalszych wyszukiwania (np. połączenie czytnika kodów kreskowych powinno umożliwiać wprowadzanie danych w celu natychmiastowego odnalezienia odpowiadającego mu materiału
* System powinien automatycznie wykrywać awarie synchronizacji sygnałów video w czasie rzeczywistym, aby zagwarantować natychmiastową detekcję awarii kamer
* System powinien także monitorować poziom kontrastu każdego wejścia video, aby natychmiast wykrywać pogorszenie obrazu kamery poprzez manipulowanie lub awarię oświetlenia.
* System powinien oferować możliwość monitorowania pola widzenia każdej kamery, aby wykrywać manipulowanie kamerami poprzez zmianę ich pozycji
* System powinien udostępniać różne algorytmy detekcji ruchu zależnie od aplikacji. Powinno być możliwe użycie różnych algorytmów dla różnych kanałów video
* System powinien zawierać podstawową detekcję aktywności video, bezpłatnie
* Konfiguracja obszaru detekcji powinna być precyzyjna i łatwa, przeprowadzana poprzez rysowanie wielokątów wewnątrz obrazu (o dowolnej ilości kątów), gdzie każdy wielokąt powinien umożliwiać skonfigurowanie różnych wartości czułości oraz wywołania alarmu w zależności od kierunku poruszania się obiektu
* Możliwość zaimplementowania dodatkowo licencjonowanej lub objętej kosztami systemu funkcji detekcji ruch specjalizowanej dla zastosowań zewnętrznych (OAD)
* Detekcja OAD powinna być dostępna dla każdej kamery i zawierać możliwość utworzenia na obrazie z kamery wirtualnego ogrodzenia z zachowaniem zasad perspektywy (pola bliżej kamery większe, pola dalej od kamery mniejsze), co umożliwi prawidłową detekcję obiektów niezależnie od ich oddalenia od punku kamerowego pod kątem wielkości jak i prędkości poruszania się .
* Algorytm OAD powinien być odporny na zjawiska pogodowe (deszcz, śnieg, cienie, zmianę jasności, wstrząsy kamery na wietrze itd.).
* Menadżer zdarzeń systemu powinien umożliwiać aktywację/dezaktywację różnych profili konfiguracji zależnych od okien czasowych lub innych akcji, również tych wyzwalanych przez samą analitykę OAD.
* System powinien być zdolny do równoczesnej aktywacji i analizy dwóch różnych metod analityk dla tej samej kamery w czasie rzeczywistym.
* Możliwość zaimplementowania dodatkowo licencjonowanej lub objętej kosztami systemu funkcji analizy obrazu, w tym analizę kierunku, prędkości poruszania się obiektów oraz ich wielkości.
* Możliwość zaimplementowania dodatkowo licencjonowanej lub objętej kosztami systemu funkcji rozpoznawania tablic rejestracyjnych.
* Dane rozpoznanych tablic rejestracyjnych z obrazem video powinny być dostępne na lokalnym DVR/NVR, ale także zdalnie ze stacji klienta.
* System udostępniać pełną funkcjonalność krosownicy wizyjnej (analogowej lub zbudowanej na bazie sieci IP) z możliwością:
  + krosowania sygnałów na żywo oraz obrazów zapisanych w bazie danych
  + krosowania kamer analogowych z kamerami IP
  + grupowe przełączanie kamer na poszczególne monitory
  + sterowanie kamerami obrotowymi
  + wyświetlanie komunikatów alarmowych
  + ustawienie sekwencji dla poszczególnych kamer
  + podgląd na poszczególnych monitorach w trybach wieloekranowych (wiele kamer obserwowanych jednocześnie w podziale ekranu na pojedynczym monitorze)
  + podłączenie wielu klawiatur
  + powinna istnieć możliwość modernizacji oprogramowania sprzętowego
  + możliwość zaprogramowania do 50 niezależnych sekwencji
  + obsługa wszystkich kamer na obiekcie musi być zapewniona w sposób płynny i stabilny oraz zapewnienie możliwości rozbudowy bez kosztowej środowiska o 30% poprzez przyłączanie dodatkowych urządzeń .

**Parametry techniczno-funkcjonane stacji operatorskiej, oprogramowania klienckiego**

* Podgląd i przeglądanie zarejestrowanych obrazów i dźwięku powinno być możliwe przy użyciu oprogramowania, dostarczonego bezpłatnie przez dostawcę cyfrowego systemu VSS na nośnikach CD-ROM lub DVD-ROM, pracującego na komputerze klasy PC.
* Stacja VSS: przystosowany do pracy ciągłej, procesor Intel CORE i7 czwartej generacji 4.00GHz, pamięć RAM 16 GB, zasilacz min 350W, dysk twardy SSD 256GB, napęd DVD/RW, klawiatura/myszka logitech, karta graficzna nvidia GT 610 (w zależności od ilości monitorów stacje należy wyposażyć w dwie takie karty graficzne) Windows 11 Pro 64 pl
* Konfiguracja stacji, musi posiadać skonfigurowane konto administratora systemu dla serwisu i zarządzania oraz konto operatora o ograniczonej funkcjonalności, skonfigurowany i uruchomione zdalny dostęp do stacji za pomocą RDP.
* Każda stacja robocza użytkownika powinna mieć nieograniczony dostęp do wielu jednostek DVR/NVR jednocześnie. Oprogramowanie do podglądu obrazów (na żywo i zarejestrowanego materiału) może być instalowane bezpłatnie na dowolnej ilości stacji podglądowych, przy czym każda z tych stacji może w dowolnym momencie połączyć się z rejestratorem (o ile nie został wykorzystany w tym konkretnym momencie limit dostępnych sesji na rejestratorze)
* Interfejs użytkownika powinien umożliwiać jednoczesne wyświetlanie obrazu z tej samej kamery, na jednym ekranie, w wielu oknach, w różnych trybach (na żywo, odtwarzanie w przód, odtwarzanie wstecz, odtwarzanie poklatkowe) jak również odtwarzanie obrazów z różnych kamer w wielu oknach podglądu.
* Interfejs użytkownika powinien umożliwiać jednoczesne wyświetlanie obrazu z wielu urządzeń rejestrujących, na jednym ekranie, w wielu oknach, w różnych trybach (na żywo, odtwarzanie w przód, odtwarzanie wstecz, odtwarzanie poklatkowe)
* Użytkownik powinien mieć możliwość ustawienia dowolnego rozmiaru, proporcji i pozycji każdego okna podglądu dzięki czemu możliwe będzie wyświetlanie niezniekształconego obrazu z dowolnej kamery zainstalowanej w systemie (minimum kamery o proporcjach [szerokość:wysokość] 4:3; 16:9, 9:16, 10:2 itd.). Domyślnie system powinien udostępniać prezentację obrazu jako regularną matrycę o 1,4,9,16,25 lub 36 okienkach podglądu oraz szablony podglądów alarmowych z podziałami 1/5, 1/7 lub 1/9 okien podglądu.
* System powinien zezwalać na określenie szczegółowych scenariuszy uruchamiania dla użytkownika lub grup użytkowników, dotyczących połączeń z predefiniowanymi serwerami oraz podglądu predefiniowanych kamer z danych serwerów, a także wywołania wcześniej zdefiniowanych (dla każdego użytkownika indywidualnie) scen z odpowiednimi kamerami tak w trybie „na żywo”, jak i odtwarzania z bazy danych (w przód, w tył, stop klatka itd.) . Poziom uprawnień określać powinien również dostęp do zarejestrowanego materiału, sterowanie kamerami obrotowymi, prawo do exportu nagrań, drukowania zdjęć itd.
* Podgląd alarmowy (wywołanie sceny po wystąpieniu alarmu) powinien umożliwiać wyświetlenia pojedynczych obrazów przed- i po-alarmowych oraz całych sekwencji obrazów w pętli, dla jednej lub wielu kamer.
* Funkcja szybkiego wyszukiwania obrazu powinna być definiowana poprzez określenie takich kryteriów wyszukiwania jak czas, data, numer kamery, typ zdarzenia, data zdarzenia, tak dla pojedynczego rejestratora jak i dla całej grupy rejestratorów włączonych w system
* Powinna istnieć możliwość wyszukiwania po detekcji ruchu na zarejestrowanym obrazie
* Ciąg danych pochodzący z czytnika kodów kreskowych (lub innego podłączonego urządzenia) powinien być udostępniony, jako kryterium wyszukiwania w celu bezpośredniego wyszukania materiału, który został zapisany z tymże ciągiem danych (kod kreskowy lub inne).
* Analiza alarmów lub zdarzeń powinna umożliwiać bezpośredni dostęp do obrazów związanych z tymi zdarzeniami, poprzez przeglądanie globalne wszystkich zdarzeń w systemie, zdarzeń przetwarzanych poprzez wybrany serwer lub zdarzeń związanych wyłącznie z wybrana kamerą.
* Wyszukiwanie obrazu w grupie kamer powinno umożliwiać późniejsze zsynchronizowane wyświetlanie wszystkich lub wybranych obrazów (za pomocą jednej komendy ustawienie kamer na ten sam czas) odpowiadające danym kryteriom wyszukiwania z różnych kamer, w różnych oknach podglądu, bez względu na liczbę jednostek DVR/NVR, z którymi połączone są kamery z danej grupy.
* Proces odtwarzania nagrań w przód/w tył powinien obsługiwać prędkości to x1, x2, x4 aż do x1000 w sposób umożliwiający płynne odtwarzanie. Szybkie i standardowe odtwarzanie w przód i w tył tylko pomiędzy ramkami kluczowymi nie jest akceptowany
* Przewijanie/cofanie po jednej klatce musi zawierać całe klatki, przeskok tylko do kluczowych klatek nie jest akceptowany.
* W przypadku wyszukiwania dotyczącego wybranej kamery, operator powinien mieć możliwość dokonania wyboru spośród listy dostępnych nagrań oraz punktu na wskaźniku czasu. Lista nagrań powinna zawierać wszystkie kamery, również te, które w obecnej chwili nie przekazują obrazu „na żywo”, a nadal posiadają obrazy wideo przechowywane w bazie danych urządzenia DVR/NVR.
* System udostępniać powinien funkcję „inteligentnego podglądu sceny”. W tym trybie wybór danej kamery powinien automatycznie wyświetlić scenę złożoną z tej kamery i kamer z jej otoczenia dając pełen przegląd sytuacji na monitorowanej scenie.
* W celu odnalezienia określonego nagrania wideo, operator nie musi wybierać odpowiedniego urządzenia nagrywającego. Użytkownikowi powinna być udostępniona jednolita lista wszystkich dostępnych kamer, niezależnie od tego, do jakiego rejestratora DVR/NVR kamery te są podłączone.
* Przy wybieraniu kamery, lista kamer do wyboru powinna być przedstawiona, jako struktura drzewa katalogowego. Różne typy kamer (stacjonarne, obrotowe, IP i inne) powinny być wyróżnione w widoku drzewa odpowiednim symbolem lub kolorem.
* W uzupełnieniu lub zamiast dedykowanego oprogramowania klienckiego, obrazy na żywo lub zarejestrowane oraz dźwięk powinny być także dostępne ze standardowych przeglądarek WEB poprzez HTML5 bez użycia specjalnych „wtyczek tzw. pluginów lub innych dodatków do przeglądarek”.
* Obsługa z przeglądarki WEB umożliwiać powinna wyszukiwanie obrazów. Wyszukiwanie to powinno być możliwe przynajmniej po czasie, dacie, numerze kamery
* Obsługa z przeglądarki WEB umożliwiać powinna oglądanie przynajmniej 9 strumieni video lub zarejestrowanych obrazów z tej samej kamery z różnych okresów czasu
* Obsługa z przeglądarki WEB umożliwiać powinna sterowanie kamerami obrotowymi
* System powinien udostępniać opcjonalny (w wersji podstawowej lub na bazie dodatkowych licencji), interaktywny, graficzny interfejs użytkownika (mapy obiektu z naniesionymi kamerami), aby umożliwić pełną kontrolę wszystkich rejestratorów DVR/NVR w graficznym systemie kontroli obrazu określonym przez użytkownika. System ten powinien zezwalać na import map w formacie standardowych obrazów systemu Windows, takich jak bmp, tiff, lub jpeg. Użytkownik powinien posiadać możliwość definiowania wyglądu oraz funkcji elementów graficznych (ikon), takich jak kamery, wejścia alarmowe oraz wyjścia przekaźnikowe. System posiadać musi możliwość tworzenia i modyfikowania przez użytkownika poszczególnych elementów (ikon).
* GUI zapewniać powinno nie tylko dostęp poprzez mapę do kamer i funkcji, ale także przedstawiać zmieniające się symbole i ikony zależnie od różnych informacji systemowych, np. symbol kamery przedstawiający poprawny lub niepoprawny status kamery, załączoną lub wyłączoną analitykę, alarm lub brak alarmu itp.
* Oprogramowanie konfiguracyjne powinno być oddzielone od oprogramowania podglądu. Powinno się je uruchomić na standardowym komputerze klasy PC z systemem Windows 11 w wersji Proffesional 64 bitowej lub nowszym.
* Połączenie oprogramowania konfiguracyjnego z jednostkami systemu powinno być możliwe lokalnie, jak również poprzez sieć (przy użyciu protokołu TCP/IP).
* System powinien posiadać opcję szyfrowania zgrywanego na nośniki zewnętrzne materiału, a także możliwość szyfrowania transmisji od serwera do stacji podglądowej
* System powinien umożliwiać tworzenie wielopoziomowego systemu zabezpieczeń dostępu w oparciu o hasła. System powinien umożliwiając tworzenie kont pojedynczych użytkowników oraz grup użytkowników z przypisanymi uprawnieniami dostępu. Prawa dostępu powinny, co najmniej umożliwić rozróżnienie grup administracyjnych (z dostępem do opcji konfiguracji systemu) oraz grup użytkowych (dostęp do poszczególnych rejestratorów i kamer, podgląd "na żywo" oraz dostęp do archiwum, definiowanie akcji takich jak przetwarzanie i wyświetlanie stanów alarmowych, tworzenie kopii zapasowych, drukowanie, eksport sekwencji obrazów).
* Stacje podglądowe posiadać powinny możliwość podłączenia min. 2 monitorów, z ich dowolną konfiguracją ( pojedyncze obrazy, podziały ekranów, monitory alarmowe itp.). Wydajność stacji pozwolić powinna na wyświetlanie minimum 400 kl/sek (dla 2 monitorów przy rozdzielczości HD) lub 800 kl/sek (dla 4 monitorów przy rozdzielczości HD).

**Parametry techniczno-funkcjonalne konsoli operatora systemu dla obsługi kamer obrotowych**

Klawiatura systemowa winna posiadać możliwość:

* Sterowania funkcjami rejestratorów oraz krosownicy wizyjnej
* Sterowania kamer obrotowych przy pomocy drążka sterującego
* Wbudowany wyświetlacz ciekłokrystaliczny
* Możliwość definiowania min 5 przycisków na klawiaturze, umożliwiając wykonywanie poleceń zaprogramowanych w systemie
* Możliwość sterowania wieloma rejestratorami z pozycji jednej klawiatury ( min. do 32 rejestratorów)
* Możliwość podłączenia do systemu za pomocą portu RS232, RS-422 lub poprzez sieć LAN

**Parametry techniczno-funkcjonalne dla kamer ogrodzeniowych**

Zintegrowana kamera szybkoobrotowa minimum 4Mpix z kamerą 4 przetwornikową – kamera referencyjna AXIS Q6135-LE

• Wbudowane zaawansowane analityki obrazy takie jak:

o Obiekt w obszarze, przekroczenie linii, czas przebywania w strefie

o Klasyfikacja obiektów wg cech: człowiek, samochód, kolor samochodu, motocykl

• Certyfikat TPM, FIPS 140-2 poziom 2

• Kamera powinna posiadać przetwornik obrazu CMOS RGB 1/2.8’’ ze skanowaniem progresywnym

• Obiektyw kamery powinien być z zakresu f=4.3 – 137,6 mm, F1.4-4.0, kąt widzenia w poziomie: 58.3° - 2.4°, w pionie 34.9° - 1.3°,

• Kamera powinna automatycznie zdejmować filtr odcinający promieniowanie podczerwone,

• Minimalne oświetlenie kamery dla trybu kolorowego powinno wynosić 0.06 luksa dla 30 IRE F1.4 oraz 0.008 luksów dla 30 IRE F1.4 dla trybu czarno-białego, 0 luksów przy włączonym oświetleniu w podczerwieni

• Obrót 360° z prędkością 0.05°-700°/s, pochylenie od +20° do -90° z prędkością 0.05°-500°/s,

• Zoom optyczny x32, zoom cyfrowy x12, łączny zoom x384,

• Kamera powinna obsługiwać kompresję wideo H.264, H.265,

• Kamera powinna mieć rozdzielczość z zakresu: HDTV 1080p 1920x1080 do 160x90 (50Hz),

• Poklatkowość kamery powinna wynosić do 50 kl/s (50Hz) przy każdej rozdzielczości,

• Kamera powinna posiadać kilka indywidualnie konfigurowanych strumieni wizyjnych w formacie H.264 oraz H.265.

• Kamera powinna mieć możliwość ustawienia obrazu w szerokim zakresie dynamicznym (WDR do 120dB), elektroniczną stabilizację obrazu, możliwość ustawienia balansu bieli, nasycenia kolorów, nakładania teksu i obrazów, 32 maski prywatności,

• Kamera powinna posiadać obudowę polimerową IP66, odporną na uderzenia IK10

• Zasilanie kamery max. 60W,

• Kamera powinna posiadać gniazdo karty pamięci SD / SDHC / SDXC

• Warunki działania kamery powinny być z zakresu temperaturowego od – 50°C do 50°C przy wilgotności względnej 10 – 100% (z kondensacją).

Punkt kamerowy nr 2 wykonać w oparciu o następującą kamerę:

Kamera szybkoobrotowa minimum 4Mpix – kamera referencyjna AXIS Q6135-LE

• Wbudowane zaawansowane analityki obrazy takie jak:

o Obiekt w obszarze, przekroczenie linii, czas przebywania w strefie

o Klasyfikacja obiektów wg cech: człowiek, samochód, kolor samochodu, motocykl

• Certyfikat TPM, FIPS 140-2 poziom 2

• Kamera powinna posiadać przetwornik obrazu CMOS RGB 1/2.8’’ ze skanowaniem progresywnym

• Obiektyw kamery powinien być z zakresu f=4.3 – 137,6 mm, F1.4-4.0, kąt widzenia w poziomie: 58.3° - 2.4°, w pionie 34.9° - 1.3°,

• Kamera powinna automatycznie zdejmować filtr odcinający promieniowanie podczerwone,

• Minimalne oświetlenie kamery dla trybu kolorowego powinno wynosić 0.06 luksa dla 30 IRE F1.4 oraz 0.008 luksów dla 30 IRE F1.4 dla trybu czarno-białego, 0 luksów przy włączonym oświetleniu w podczerwieni

• Obrót 360° z prędkością 0.05°-700°/s, pochylenie od +20° do -90° z prędkością 0.05°-500°/s,

• Zoom optyczny x32, zoom cyfrowy x12, łączny zoom x384,

• Kamera powinna obsługiwać kompresję wideo H.264, H.265,

• Kamera powinna mieć rozdzielczość minimum z zakresu: HDTV 1080p 1920x1080 do 160x90 (50Hz),

• Poklatkowość kamery powinna wynosić do 50 kl/s (50Hz) przy każdej rozdzielczości,

• Kamera powinna posiadać kilka indywidualnie konfigurowanych strumieni wizyjnych w formacie H.264 oraz H.265.

• Kamera powinna mieć możliwość ustawienia obrazu w szerokim zakresie dynamicznym (WDR do 120dB), elektroniczną stabilizację obrazu, możliwość ustawienia balansu bieli, nasycenia kolorów, nakładania teksu i obrazów, 32 maski prywatności,

• Kamera powinna posiadać obudowę polimerową IP66, odporną na uderzenia IK10

• Zasilanie kamery max. 60W,

• Kamera powinna posiadać gniazdo karty pamięci SD / SDHC / SDXC

• Warunki działania kamery powinny być z zakresu temperaturowego od – 50°C do 50°C przy wilgotności względnej 10 – 100% (z kondensacją).

**Parametry techniczno-funkcjonalne dla kamer obrotowych**

* Kamera powinna posiadać przetwornik obrazu CMOS 1/2’’ ze skanowaniem progresywnym.
* 31-krotny zoom optyczny, 12-krotny zoom cyfrowy
* Obiektyw kamery powinien być min. z zakresu f=7 – 214 mm, F1.36-4. Kąt widzenia w poziomie: min. z zakresu 60.6° - 2.0°, kąt widzenia w pionie min. z zakresu 36.5° - 1.1°.
* Kamera powinna automatycznie usuwać filtr odcinający promieniowanie podczerwone.
* Laserowe ustawianie ostrości
* Minimalne oświetlenie kamery dla trybu kolorowego powinno wynosić min. 0.06 luksa przy 30 IRE F1.36 oraz 0 luksów przy włączonym oświetlaczy podczerwieni dla trybu czarno-białego.
* Czas otwarcia przesłony kamery powinien być z zakresu min. 1/111 000 s do 1/2 s.
* Kamera powinna umożliwiać zaprogramowanie min. Szybkizoom, adirflip, 300prepozycji, rejestracja trasy (maks. 10 tras, maks. szas trwania każdej trasy: 16minut), trasa strażnika (maks. 100tras), kolejka sterowania, ekranowy wskaźnik kierunku, ustawianie nowego obrotu,regulowana prędkość zoomu, szybkie suszenie (speeddry)
* Kamera powinna obsługiwać kompresję wideo H.265, Motion JPEG.
* Kamera powinna mieć rozdzielczość minimum z zakresu minimum: HDTV 1080p 1920x1080 do 320x180.
* Poklatkowość kamery dla kompresji H.265 powinna wynosić do 25 kl/s przy każdej rozdzielczości.
* Kamera powinna umożliwiać indywidualną konfigurację wielu osobnych strumieni obrazu wideo w formacie H.265 wraz z regulacją szybkości klatek i przepustowością VBR/MBR H.265.
* Kamera powinna mieć możliwość ustawienia obrazu w szerokim zakresie dynamicznym (WDR), ręcznym czasie migawki, kompresji, kolorze, jasności, ostrości, balansu bieli, regulacji ekspozycji, strefy ekspozycji, kompensacji podświetlenia, dokładnym ustawieniu zachowania przy słabym oświetleniu, obrocie, nakładaniu tekstu i obrazu, min. 32 indywidualnych masek prywatności, zatrzymania obrazu w PTZ, elektronicznej stabilizacji obrazu.
* Kamera powinna obsługiwać protokoły m.in.: IPv4/v6, HTTP, HTTPSa, SSL/TLSa, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnPTM, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SFTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH, NTCIP
* Kamera powinna posiadać obudowę aluminiową IP66, przezroczystą kopułkę z poliwęglanu, osłonę przeciwsłoneczną.
* Kamera powinna mieć złącze RJ45 do 10BASE-T/100BASE-TX PoE.
* Kamera powinna posiadać gniazdo karty pamięci SD/SDHC/SDXC o pojemności do 64 GB.
* Warunki działania kamery powinny być z min. zakresu temperaturowego od – 50°C do 50°C, przy wilgotności względnej 10 – 100% ( z kondensacją).

**Parametry techniczno-funkcjonalne dla kamer stałopozycyjnych zewnętrznych**

* Kamera powinna posiadać przetwornik obrazu CMOS 1/2.8’’ ze skanowaniem progresywnym
* Obiektyw kamery powinien być z zakresu f=2.8 – 8 mm, F1.2. Kąt widzenia w poziomie: 107° - 42°, w pionie 57° - 24°.
* Kamera powinna automatycznie zdejmować filtr odcinający promieniowanie podczerwone.
* Minimalne oświetlenie kamery dla trybu kolorowego powinno wynosić 0.05 luksa dla 50 IRE F1.2 oraz 0.01 luksów dla 50 IRE F1.2 dla trybu czarno-białego.
* Czas otwarcia przesłony kamery powinien być z zakresu 1/66500 s do 2 s.
* Kamera powinna obsługiwać kompresję wideo H.265.
* Kamera powinna mieć rozdzielczość z zakresu minimum: HDTV 1080p 1920x1080 do 160x90.
* Poklatkowość kamery dla kompresji H.265 powinna wynosić do 25 kl/s przy każdej rozdzielczości.
* Kamera powinna umożliwiać indywidualną konfigurację wielu osobnych strumieni obrazu wideo w formacie H.265 wraz z regulacją szybkości klatek i przepustowością VBR H.265.
* Kamera powinna mieć możliwość ustawienia obrazu w szerokim zakresie dynamicznym (WDR), kompresji, kolorze, jasności, ostrości, balansu bieli, kompensacji oświetlenia tylnego, dokładnej regulacji działania w warunkach słabego oświetlenia, nakładaniu tekstu i obrazu, maski prywatności, mirroringów obrazów.
* Kamera powinna obsługiwać protokoły m.in.: IPv4/v6, HTTP, HTTPS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPN-ENP, SNMPv1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH.
* Kamera powinna posiadać obudowę polimerową IP66, odporną na uderzenia.
* Zasilanie kamery powinno być zgodne z normą IEEE 802.3af/802,3at Typ 1, Klasa 3, max. 12.95W
* Kamera powinna mieć złącze RJ45 do 10BASE-T/100BASE-TX PoE,
* Kamera powinna posiadać gniazdo karty pamięci SD/SDHC/SDXC
* Warunki działania kamery powinny być z zakresu temperaturowego od – 40°C do 60°C przy wilgotności względnej 10 – 100% RH ( z kondensacją).

**Parametry techniczno-funkcjonalne dla kamer stałopozycyjnych, kopułkowych wewnętrznych**

* Kamera powinna posiadać przetwornik obrazu CMOS 1/2,8’’ ze skanowaniem progresywnym
* Obiektyw kamery powinien być z zakresu f=3,4 – 8,9 mm, F1.8. Kąt widzenia w poziomie: 100° - 36°, w pionie 53° - 20°.
* Kamera powinna automatycznie zdejmować filtr odcinający promieniowanie podczerwone.
* Minimalne oświetlenie kamery dla trybu kolorowego powinno wynosić 0.1 luksa dla F1.8 oraz 0.00 luksów dla F1.8 dla trybu czarno-białego i włączonym oświetlaczu IR
* Czas otwarcia przesłony kamery powinien być z zakresu 1/66500 s do 2 s.
* Kamera powinna obsługiwać kompresję wideo H.265.
* Kamera powinna mieć rozdzielczość z zakresu minimum : HDTV 1080p 1920x1080 do 160x90.
* Poklatkowość kamery dla kompresji H.265 powinna wynosić do 25 kl/s przy każdej rozdzielczości.
* Kamera powinna umożliwiać indywidualną konfigurację wielu osobnych strumieni obrazu wideo w formacie H.265 wraz z regulacją szybkości klatek i przepustowością VBR H.265.
* Kamera powinna mieć możliwość ustawienia obrazu w szerokim zakresie dynamicznym (WDR), kompresji, kolorze, jasności, ostrości, balansu bieli, kompensacji oświetlenia tylnego, dokładnej regulacji działania w warunkach słabego oświetlenia, nakładaniu tekstu i obrazu, maski prywatności, mirroringów obrazów.
* Kamera powinna obsługiwać protokoły m.in.: IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPNP, SNMPv1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH.
* Kamera powinna posiadać obudowę odporną na uderzenia w klasie IK-10.
* Zasilanie kamery powinno być zgodne z normą IEEE 802.3af/802.3at Typ 1, Klasa 3, max. 8,9W
* Kamera powinna mieć złącze RJ45 do 10BASE-T/100BASE-TX PoE
* Kamera powinna posiadać gniazdo karty pamięci SD/SDHC/SDXC
* Warunki działania kamery powinny być z zakresu temperaturowego od 0°C do 50°C przy wilgotności względnej 10 – 85% RH (bez kondensacji).

**Parametry techniczno-funkcjonalne dla kamer termowizyjnych zewnętrznych**

* Kamera powinna być wyposażona w niechłodzony mikrobolometr o rozdzielczości minimum 640x480 i rozmiarze piksela: 17µm
* Kamera powinna zapewniać obrazy termowizyjne o czułości NETD mniejsze lub równe 30 mK
* Kamera powinna dostarczać konfigurowane strumienie wideo w formatach Motion JPEG i H.265.
* Obsługiwać powinna rozdzielczość 640x480, po przeskalowaniu 800x600 pixeli.
* Kamera posiadać powinna wbudowaną i możliwą do użytkowania bez dodatkowych licencji funkcję wideo detekcji ruchu, zabezpieczenie antysabotażowe.
* Kamera posiadać powinna możliwością zasilania poprzez Ethernet.
* Kamera posiadać powinna wbudowane gniazdo kart pamięci,
* Kamera powinna być przeznaczona do pracy w temperaturach od -40 do +60°C.
* Klasa ochrony minimum IP66.
* Kamera powinna obsługiwać zarówno statyczne adresy IP, jak i te z serwera DHCP oraz protokoły IPv4 i IPv6. Kamera powinna obsługiwać funkcję Quality of Service(QoS).
* Dla zapewnienia bezpiecznego dostępu do kamery i przesyłanej zawartości, kamera powinna obsługiwać szyfrowanie HTTPS i uwierzytelnianie IEEE802.1X.
* Kamera powinna obsługiwać otwarty i opublikowany interfejs API.

**System sygnalizacji włamania i napadu**

Zadaniem systemu SSWIN w zakresie stref ochrony: peryferyjnej oraz wewnętrznej Elektrowni jest bezpośrednie wsparcie pracowników ochrony fizycznej w realizacji zadań służbowych m.in. szybkiej identyfikacji zagrożenia i jego eliminacji po prawidłowej ocenie.

Jako obiekt infrastruktury krytycznej IK poszczególne budynki techniczne i administracyjne na terenie przedmiotowych obiektów należy objąć systemami włamania i napadu w stopniu zabezpieczenia 2 lub 3 w zależności od analizy ryzyka. System sygnalizacji włamania i napadu należy wykonać jako rozbudowę istniejącego systemu SSWiN przy zachowaniu pełnej integracji z istniejącymi systemami: zarządzania bezpieczeństwem PSIM, kontroli dostępu SKD oraz monitoringu wizyjnego VSS przy użyciu dedykowanych interfejsów sprzętowo-programowych oraz wzajemnych zasterowań.

Jako urządzenia detekcji intruza należy zastosować następujące elementy:

* system ochrony napłotowej,
* czujki PIR,
* czujki MW,
* czujki stłuczeniowe,
* piloty napadowe,
* przyciski napadowe nożne,
* bariery mikrofalowe,
* magnetyczne czujniki otwarcia.

Sygnalizacja alarmu włamania i napadu zrealizaować w następujący sposób:

* poprzez sygnalizatory optyczno-akustyczne,
* wizualizację w systemie SZB.

Zasterowania między SSWIN a SKD zrealizować w oparciu o:

* min. nadzór nad sygnałami użycia przycisku awaryjnego, siłowego wejścia SKD, braku 230 VAC, awarii akumulatora i sabotażu układu zasilania SKD.

Zasterowania między SSWIN a systemem napłotowym zrealizować w oparciu o:

* min. nadzór nad sygnałami alarmu z grupy systemu napłotowego, braku 230VAC, awarii akumulatora, sabotażu układu zasilania systemu napłotowego.

**Parametry techniczno-funkcjonalne systemu SSWIN**

* centrala w 3 stopniu zabezpieczenia zgodnym z normą PN-EN50131-1
* urządzenia detekcyjne w 2 stopniu zabezpieczenia zgodnym z normą PN-EN50131-1
* wbudowany, w pełni monitorowany zasilacz impulsowy o wydajności min. 2,5A
* minimalna liczba linii dla całego systemu: 520
* minimalna liczba linii na płycie centrali alarmowej: 16
* minimalna liczba wyjść 400mA na płycie centrali alarmowej: 8
* minimalna liczba klawiatur w systemie: 32
* minimalna liczba użytkowników: 999

**System Kontroli Dostępu KD**

Kontrola przejścia w obiektach infrastruktury krytycznej IK jest kluczowym elementem zabezpieczenia, porządkującym nie tylko ruch na obiekcie, wymuszając zgodne z polityką bezpieczeństwa Zakładu zachowana pracowników oraz osób nie będących pracownikami, tzn. gości, ale również stanowi środek prewencyjny przed potencjalnym zagrożeniem ze strony napastnika, intruza, gdyż stanowi środek utrudniający swobodne przemieszczanie się.

Stan każdego z wejścia objętego systemem KD zwizualizować w systemie SZB przy wykorzystaniu interfejsu programowego oraz oprogramowaniu KD na jednostkach administratorów systemu KD i SZB.

Systemu kontroli dostępu zainstalować w oparciu o:

* kontroler dostępu, obsługujący dwa przejścia, z wbudowanym zasilaczem buforowym,
* czytniki zbliżeniowe HID i karty, w standardzie iClass SE,
* akumulator 12 V,
* przycisk ewakuacyjny,
* zwora elektromagnetyczna, z kontrolą stanu,
* samozamykacz,
* oprogramowanie zarządzające,
* serwer.

W celu uzyskania funkcjonalności rejestracji czasu pracy przy wykorzystaniu projektowanej struktury systemu kontroli dostępu należy system kontroli dostępu wyposażyć w:

* rejestratory czasu pracy z wbudowanym czytnikiem HID, w standardzie iClass SE w przejściach kontrolowanych oznaczonych jako przejścia RCP,
* interfejs SAP (System Administracji Przedsiębiorstwem) dla oprogramowania zarządzającego systemu kontroli dostępu.

W systemie kontroli dostępu należy zdefiniować przejścia objęte funkcjonalnością RCP. Baza danych systemu KD na potrzeby RCP poprzez interfejs programowy powinna generować format danych wymagany przez system SAP. Rozliczenie czasu pracy pracowników nie jest przedmiotem systemu kontroli dostępu, który pozostaje w gestii dotychczasowego systemu SAP.

Systemem kontroli dostępu należy zrealizować w stopniu zabezpieczenia min. 2. System SKD należy wykonać jako rozbudowę systemu SKD funkcjonującego w EC Szczecin i EC Pomorzany przy zachowaniu pełnej integracji z systemami: zarządzania bezpieczeństwem PSIM, systemem sygnalizacji włamania i napadu SSWIN oraz monitoringu wizyjnego VSS przy użyciu dedykowanych interfejsów sprzętowo-programowych.

**Parametry techniczno-funkcjonalne dla systemu SKD**

* System kontroli dostępu musi spełniać wymagania min. stopnia zabezpieczenia 2 wg PN-EN 60839-11-1:2014-01/AC potwierdzone deklaracją zgodności z ww. normą.
* Sterownik powinien pracować w zakresie napięcia zasilania od 12-14 VDC.
* Sterownik powinien pracować w oparciu o płytę główną dwuprocesorową, z maksymalnym poborem pradu 350mA, pamięcią RAM min. 2 MB oraz pamięcią wewnętrzną flash min. 2GB.
* Sterownik powinien posiadać następujące interfejsy:
  + Min. 1x Ethernet – przeznaczony do personalizacji instalacji za pomocą strony www oraz komunikacji z oprogramowaniem zarządzającym za pomocą szyfrowanego połączenia TCP/IP
  + Min. 1x RS-232/RS-485 -do konfiguracji sterownika
  + Min. 1x RS-232 – do urządzeń peryferyjnych
  + Min. 1x separowany galwanicznie interfejs CAN do podłączenia modułów rozszerzeń
  + Min. 4x AbaTrackII/Wiegand
  + Min. 8x uniwersalne wejścia/wyjścia – umożliwiające podłączenie czujek alarmowych
  + Min. 2x uniwersalny port rozszerzeń – umożliwiające wpięcie dodatkowych portów
  + Min. 1x port UI – umożliwiający podłączenie klawiatury i wyświetlacza.
  + Min. 1x port CAN (poziomy TTL) nieseperowany
* Sterownik powinien obsługiwać min. 2 złącza punktu kontroli dostępu, min. 16 modułów rozszerzeń podłączonych za pomocą magistrali CAN
* Sterownik powinien posiadać wejścia:
  + Min. 2x przycisk otwarcia drzwi
  + Min. 2x kontaktron
  + Min. 4x sabotaż czytnika
  + Min. 1x sabotaż sterowniaka
  + Min. 1x info o zasilaniu
  + Min. 1x alarm PPOŻ (optoizolowane)
* Sterownik powinien posiadać wyjścia:
  + Min. 2x wyjście rygiel (przekaźnik NO/NC 30V/1A)
  + Min. 2x wyjście alarmowe (przekaźnik NO/NC 30V/1A)
  + Min. 3x wyjście Vout (każde max 1 A)
  + Min. 1x wyjście Vout (max 500mA) przy interfejsie RS232 (LS2)
  + Min. 1x wyjście 5V (max 500 mA) przy interfejsie RS484 (LS5)
* Sterownik powinien być zamontowany w obudowie metalowej, nie przekraczać wagi 2,5 kg.
* Sterownik powinien określać czas na podstawie zegaru czasu rzeczywistego (RTC) w systemie 24h.
* Sterownik powinien mieć potrzymanie bateryjne pamięci RAM i zegara.
* Sterownik powinien pracować w zakresie temperatur min. od -10° do 55°C, przy wilgotności względnej otoczenia poniżej 80% bez kondensacji.

**Parametry techniczno-funkcjonalne dla stacji operatorskiej systemu SKD, oprogramowania klienckiego**

Administrowanie i zarządzanie systemem KD powinno być możliwe przy użyciu oprogramowania, pracującego na komputerze klasy PC.

* Stacja operatorska systemu KD powinna być przystosowana do pracy ciągłej i wyposażona min. w: Windows 11, procesor Intel CORE i7 czwartej generacji 4.00GHz, pamięć RAM 16 GB, zasilacz min 350W, dysk twardy SSD 256GB, napęd DVD/RW, uprawnienia administratora przy instalacji.
* Stacja serwerowa – zakłada się uruchomienie w środowisku wirtualnym wOT udostępnionym przez Zmawiającego
* Konfiguracja stacji, musi posiadać skonfigurowane konto administratora systemu dla serwisu i zarządzania oraz konto operatora o ograniczonej funkcjonalności, skonfigurowany i uruchomione zdalny dostęp do stacji za pomocą RDP i VNC
* oprogramowanie musi zapewniać:
  + intuicyjną obsługę
  + bezpieczeństwo
  + automatyczne reakcję na zdarzenia
  + graficzną wizualizację
  + wbudowany wewnętrzny komunikator
  + szerokie możliwości raportowania
  + raporty przez WWW
  + obsługę urządzeń biometrycznych.

**Wydzielona sieć teleinformatyczna na potrzeby systemów bezpieczeństwa SEC-LAN;**

Dla zapewnienia poprawnej pracy elektronicznych systemów bezpieczeństwa, jak również zapewnienia bezpieczeństwa fizycznego dla pracy urządzeń w ramach tych systemów należy wykonać, wydzieloną sieć SECURITY LAN, w oparciu o okablowanie poziome min. U/UTP kat. 6A, okablowanie pionowe światłowodowe, jednomodowe oraz urządzenia aktywne, m.in. switche zarządzalne min. 1 Gb/port, 2xSFP zgodnie z przyjętymi standardami tj. : Zał.\_B8D Wytyczne szczegółowe dla budowy nowych sieci LAN w obiektach GK PGE-v2-2022 oraz Zał.\_B8A CIO-STD-2022-04

Punkty dystrybucyjne stanowią centra komunikacji, gromadzenia danych, zarządzania i dystrybucji zasilania dla elektronicznych systemów bezpieczeństwa. Pośrednie punkty dystrybucyjne należy wykonać wykorzystując szafy metalowe o wymiarach minimum 800x800x300 o stopni szczelności min. IP66 z płytą montażową.

* cześć elektryczną 230 VAC:
* rozłącznik główny izolacyjny, dwubiegunowy,
* rozłącznik bezpiecznikowy, dwubiegunowy,
* wkładka bezpiecznikowa,
* ogranicznik przepięć,
* lampka kontrolna pojedyncza,
* wyłącznik nadprądowy 1 biegunowy,
* moduły RDC z członem nadprądowym,
* gniazdo z bolcem,
* przekaźnik,
* gniazdo przekaźnika,
* moduł warystorowy,
* listwy zaciskowe,
* część zasilania napięcia stałego 48 VDC:
* zasilacz buforowy,
* przetwornica napięcia 48 VDC na 12 VDC,
* akumulatory 12 VDC,
* część ochrony przeciwprzepięciowej torów sygnałowych UTP:
* panel przeciwprzepięciowy,
* cześć teletechniczna:
* przemysłowy przełącznik sieciowy,
* PPD kontroler – mikroprocesorowy kontroler punktu dystrybucyjnego,
* część zabezpieczenia przed nieuprawnioną manipulacją:
* czujka magnetyczno – wibracyjna,
* wkładki patentowe,
* obudowy wkładki patentowej,
* część organizacyjno – montażowa:
* panel krosowy,
* przełącznica światłowodowa, montaż na szynę TH35
* szyna DIN typ TH35,
* koryto grzebieniowe.

W pomieszczeniach serwerowni oraz węzłów IT stosować rozwiązania 19” dla zabudowy punktów PPD.

Wszystkie punkty dystrybucyjne oraz słupy oznaczyć grawerowanymi tabliczkami oznaczeniowymi. W punktach dystrybucyjnych oraz rozdzielnicach należy umieścić zalaminowane schematy logiczne, schematy elektryczne oraz widoki wyposażenia.

**Parametry techniczno-funkcjonalne dla:**

**Zarządzalny switch przemysłowy z PoE**

* 8x 10/100/1000Tx IEEE 802.3at/af, 2x 100/1000 SFP
* Redundancja połączeń: RSTP, G.8032 ERPS (Recovery Time <50ms)
* Konfiguracja: konsola Web, Telnet, CLI
* Obsługa IGMP v1/v2, do 256 grup
* Wsparcie dla QoS (IEEE802.1p) i CoS/ToS
* Obsługa IEEE802.1Q VLAN, SNMP v1/v2c
* Funkcja PoE Ping Alarm
* Redundantne zasilanie 48~55VDC
* Aluminiowa obudowa ze stopniem ochrony IP30
* Temperatura pracy: -10° to 70° C
* Montaż na ścianie lub szynie DIN

**System monitorowania parametrów środowiskowych punktów dystrybucyjnych PPD**

W ramach zadania należy wykonać rozbudowę istniejącego systemu zarządzania parametrami środowiskowymi pracy dla punktów dystrybucyjnych PPD. System ma nadzorować ciągłość obecności zasilania podstawowego, temperatury oraz wilgotności wewnątrz punktu PPD a także wykrywać próby sabotażu (otwarcie, uderzenia w obudowę).

**Parametry techniczno-funkcjonalne dla urządzenia kontrolnego – Mikroprocesorowy kontroler punktu dystrybucyjnego – PPD kontroler:**

* Urządzenie powinno posiadać następujące funkcjonalności oraz właściwości techniczno-użytkowe:
* Przekazywanie alarmów do zintegrowanych systemów nadzoru: m.in. system zarządzania bezpieczeństwem PSIM, system zarządzania monitoringiem wizyjnym VSS.
* Alarmowanie o przekroczeniu predefiniowanych progów temperatury i wilgotności.
* Zabezpieczenie dostępu 4 cyfrowym hasłem z możliwością przypisywania haseł jednorazowych.
* Brak wprowadzonego hasła dostępu w określonym czasie lub 3-krotne wpisanie błędnego hasła skutkuje alarmem dźwiękowym.
* Możliwość programowej konfiguracji sposobu wizualizacji i sygnalizacji dźwiękowej alarmów i awarii.
* Możliwość zdalnego rozbrojenia urządzenia.
* Zarządzanie zmianą haseł kontrolera z poziomu systemu zarządzania bezpieczeństwem PSIM.
* Automatyczne uzbrojenie urządzenia przy zamknięciu drzwi oraz po upływie zadanego czasu bezczynności.
* Szyfrowana transmisja danych (algorytm AES) wraz z autoryzacją dostępu.
* Synchronizacja z serwerem czasu.
* Funkcja zdalnej aktualizacji oprogramowania.
* Możliwość wysterowania dowolnych urządzeń wyjściowych (wentylator, grzałka).
* Alarmowanie na podstawie zmiany stanu wejść cyfrowych.
* Możliwość tworzenia zależności logicznych pomiędzy wejściami a wyjściami cyfrowymi.
* Wygaszenie ekranu na podstawie wejścia cyfrowego.
* Kontrola parametrów środowiskowych(termostat).
* Możliwość zdalnej konfiguracji parametrów sieci LAN.
* Automatyczne wyszukiwanie urządzeń w sieci LAN.
* Dedykowane oprogramowanie do konfiguracji urządzenia.
* Monitorowanie kontrolowanych parametrów, zdarzeń i alarmów, prezentacja ich na wyświetlaczu oraz przekazanie ich do zintegrowanych systemów, w tym:
  + otwarcia drzwi szafy/obudowy – obsługa czujników otwarcia,
  + wartości aktualnej temperatury i wilgotności powietrza – czujniki zintegrowane wewnętrzne i opcjonalne zewnętrzne,
  + nieuprawnionego dostępu do kontrolowanego punktu,
  + braku zasilania szafy,
  + stanu połączenia z siecią LAN,
  + stanu zdalnego połączenia z urządzeniem.
* Integracja z istniejącym zespołem rejestratorów cyfrowych VSS oraz systemem zarządzania bezpieczeństwem PSIM, w odpowiedniej konfiguracji powinna umożliwiać:
  + wywoływanie zdefiniowanych zdarzeń na podstawie alarmu z urządzenia,
  + monitorowanie parametrów urządzenia i wyświetlanie na kanale mediów,
  + ustawienie presetu kamery na miejsce zdarzenia przy wywołanym alarmie,
  + tworzenie wykresów z wykonanych pomiarów i wyświetlanie na kanale mediów,
  + sterowanie wirtualnymi wejściami/wyjściami powiązanymi z wejściami w urządzeniu,
  + wyświetlenie na urządzeniu statusu kamer.
* Wymagane parametry techniczne:
  + Dodatkowo możliwość integracji z innymi systemami poprzez dedykowany szyfrowany protokół TCP/IP.
  + Wyświetlacz kolorowy min. 3,5” o rozdzielczości min. 320x240.
  + Buzzer wysokotonowy
  + Obsługa protokołu 1-wire: dla dodatkowych, zewnętrznych czujników np. temperatury
  + Min. 3 wejścia cyfrowe
  + Min. 2 wyjścia przekaźnikowe niskonapięciowe
  + Złącze Ethernet 10/100 Base-T
  + Pamięć operacyjna flash min. 2MB
  + Pamięć EPROM min. 2048B
  + Czujnik temperatury i wilgotności
  + Temperatura pracy od -40 do +70 st.C
  + Zasilanie PoE 35-60VDC lub 5VDC lub 12VDC
  + Mocowanie na szynie DIN

**System wizualizacji i zarządzania bezpieczeństwem PSIM (Physical Security Informaction Management).**

W zakresie inicjatywy jest integracja Wszystkich Systemów Zabezpieczenia Technicznego w przedmiotowej inwestycji z istniejącym systemem PSIM Zamawiającego.

Ilość elementów modernizowanych systemów bezpieczeństwa zlokalizowanych na terenie Zakładu oraz liczba generowanych przez nie informacji wymaga uporządkowania, nadania hierarchii ważności oraz czytelnego przedstawienia wraz z podaniem precyzyjnych instrukcji dla operatora.

Zrozumiałe i szybkie wytyczne dla operatora w chwili pojawienia się sytuacji zagrożenia nie tylko nie powodują wzrostu zdenerwowania lub paniki ze strony operatora systemu, ale stanowią wręcz sposób na szybkie zażegnanie zagrożenia lub chociażby na pokierowanie innymi służbami niwelującymi to zagrożenia, np. procesu technologicznego.

Wymaga to zastosowania systemu inteligentnego zarządzania bezpieczeństwem tzw. systemu PSIM. System powinien pozwolić na łatwe wdrożenie i zapewnić poprawę bezpieczeństwa obiektów Zakładu, ludzi i procesów technologicznych. Powinien umożliwić on stałą rozbudowę i dostosowywanie do aktualnych potrzeb dyspozytorów, służb ochrony i obsługi technicznej obiektów i nadzoru Zakładu.

Wszystkie elementy elektronicznych systemów bezpieczeństwa i ich stan należy zwizualizować w systemie PSIM, w oparciu o nowe plany zagospodarowania terenu, rzuty kondygnacji, polecenia, instrukcje oraz wzajemne interakcje.

Na potrzeby obsługi obszaru Zakładu przewidziano rozbudowę systemu zarządzania bezpieczeństwem i wizualizacji SZB. W ramach realizacji niniejszego zadania, należy system PSIM:

* Doposażyć w niezbędne interfejsy programowe systemów bezpieczeństwa
* Opracować nową aplikację graficzną oraz nawigacje, uwzględniające systemy bezpieczeństwa przewidziane do wykonania w zakresie zadania,

Uwaga: Należy zapewnić pełną integralność i spójność na poziomie sprzętowym i programowym z zaprojektowanym na obiekcie systemem zarządzania bezpieczeństwem SZB. Prowadzone prace nie mogą zakłócić ciągłości pracy oraz integralności istniejących instalacji bezpieczeństwa.

**Parametry techniczno-funkcjonalne dla systemu PSIM**

* System zarządzania musi być neutralny wobec producentów integrowanych systemów i urządzeń.
* System zarządzania musi posiadać Aprobatę Techniczną, Certyfikat Zgodności i Świadectwo dopuszczenia do stosowania w ochronie przeciwpożarowej wydane przez CNBOP, w ramach której system zarządzania budynkiem realizuje współdziałanie następujących urządzeń i systemów ochrony przeciwpożarowej budynku :
  + Centrale wykrywania i sygnalizacji pożaru
  + Przeciwpożarowe klapy odcinające, klapy odcinające wentylacji pożarowej oraz inne elementy systemów wentylacji pożarowej (np. wentylatory oddymiające);
  + Systemy wentylacji grawitacyjnej (klapy i okna oddymiające)
  + Systemy oświetlenia awaryjnego;
  + Elementy oddzieleń pożarowych (drzwi, kurtyny, bramy);
  + Urządzenia i systemy stałych urządzeń gaśniczych;
  + Inne systemy, instalacje i urządzenia wykorzystywane lub sterowane w czasie stanu alarmu pożarowego (np. dźwigi pożarowe, schody ruchome, przejścia objęte kontrolą dostępu, itd.)

* System musi składać się z oprogramowania i urządzeń, dopuszczonych do stosowania w ochronie przeciwpożarowej,
* Oprogramowanie musi mieć budowę modułową. Wymiana dowolnego modułu programowego nie może wstrzymywać pracy pozostałych funkcji
* System musi współpracować z magistralą kart wejść i wyjść przeciwpożarowych komunikujących się między sobą za pomocą szyfrowanego protokołu (np. AES)
* System musi umożliwiać nadzorowanie i sterowanie siłownikami cyfrowymi za pomocą protokołu MP-Bus. System musi być certyfikowany w zakresie implementacji tego protokołu przez producenta.
* W systemie PSIM wymagane są następujące sposoby połączeń :
  + Wyjścia przekaźnikowe różnych urządzeń i systemów do wejść systemu integracyjnego,
  + Przekaźniki systemu integracyjnego do wejść sterujących różnych urządzeń i systemów,
  + Port komunikacyjny centrali integrowanego systemu do sterownika systemu integrującego
  + Port komunikacyjny integrowanych urządzeń do sterownika będącego elementem systemu integracyjnego. Dodatkowo wymaga się aby sterowniki systemu integracyjnego mogły pracować w sieci.
  + Port komunikacyjny integrowanego systemu do portu szeregowego lub gniazda Ethernet komputera systemu integracyjnego.
* System powinien pracować w sieci komputerowej oraz umożliwiać obsługę za pomocą przeglądarki internetowej z dowolnego miejsca w budynku,
* Wymagana jest możliwość pomiaru wielkości fizycznych typu ciągłego (np. prąd ładowania baterii, wartość napięcia, temperatury, ciśnienia itp.) z wymaganą częstotliwością nie mniejszą niż 1 Hz. Wymagana jest możliwość generowania alarmów na podstawie przekroczenia progów alarmowych
* Oprogramowanie musi mieć możliwość pracy w środowiskach wirtualnych
* Zdarzenia i reakcje na zdarzenia muszą być zapamiętywane w logu działań.
* Wymagane są rozbudowane systemy poziomów dostępu dla poszczególnych grup użytkowników z możliwością zróżnicowania uprawnień dostępu do :
  + Raportów
  + Procedur alarmowych
  + Planów sytuacyjnych
  + Ustawień ogólnych
  + Opracowywania i zamykania zdarzeń alarmowych, zamykania zdarzeń nieopracowanych,
  + Przekazywania zdarzeń do innych stacji obsługi ze zróżnicowaniem uprawnień na :brak dostępu, tylko odczyt, edycję, wprowadzanie nowych, kasowanie
* System powinien posiadać możliwość przypisywania uprawnień dla operatorów z możliwością tworzenia indywidualnych stanowisk obsługi przypisanych do operatora bądź grupy. (+ nadawanie uprawnień indywidualnie dla każdego elementu w Systemie). Operator na starcie powinien mieć możliwość wyboru jezyka obsługi.
* Wymagana jest możliwość skonfigurowania systemu z wieloma stanowiskami roboczymi.
* Wymagana jest możliwość logowania się do systemu z różnym poziomem obsługi.
* Wymagana możliwość skonfigurowania automatycznego kierowania zdarzeń alarmowych na odpowiednie stanowiska robocze. Dodatkowo wymagana jest możliwość przekazania zdarzenia przez użytkownika. Wymagany jest przy tym mechanizm weryfikacji czy wybrane stanowisko jest aktywne. Przy przekazywaniu zdarzenia wyświetlane są tylko aktywne stanowiska z identyfikatorem (loginem) użytkownika.
* Wymagana jest możliwość dowolnego ustawiania kategorii zdarzeń połączona z możliwością kierowania zdarzeń na stanowiska robocze. Wymagane jest zróżnicowanie kolorów zdarzeń poszczególnych kategorii.
* Zdarzenia muszą być prezentowane na liścia zdarzeń w jednowierszowej postaci zwięzłej. Musi istnieć możliwość edycji postaci zwięzłej – wymagana jest możliwość wyboru wyświetlanych danych spośród : lp. czas i data, nazwa (lokalizacja), zdarzenia, stan obecny, priorytet, kategoria, status, użytkownik
* Wymagana jest możliwość ustawienia kolejności wyświetlania zdarzeń alarmowych przynajmniej według (lp., czasu, identyfikatora czujnika, zdarzenia, priorytetu, kategorii) rosnąco lub malejąco
* Wymagane są liczniki zdarzeń oddzielne dla zdarzeń wszystkich kategorii. Musi istnieć możliwość filtrowania widoku zdarzeń na liście (stosie) alarmów na zdarzenia wybranej kategorii poprzez prostą operację (np. kliknięcie)
* Z widoku, w którym prezentowane są tylko zdarzenia wybranej kategorii (widok filtrowany) system MUSI powracać automatycznie do widoku zdarzeń wszystkich kategorii (widok nie filtrowany) po upływie zadanego czasu
* Wymagana jest możliwość korelacji zdarzeń i generowania zdarzenia dodatkowego
* Wymagana jest możliwość wykonywania backupu online oraz backupu przyrostowego. Możliwość backupu bazy danych. Możliwość odtworzenia systemu z backupu
* Wymagana jest sygnalizacja przerwy komunikacji z każdym integrowanym systemem poprzez wyświetlenie odpowiedniego komunikatu alarmowego
* Wymagane jest, że system PSIM musi automatycznie powrócić do stanu pracy. Niezbędne składniki oprogramowania (moduły) muszą być uruchamiane automatycznie (np. usługi systemu operacyjnego).
* Powinien umożliwiać wizualizację i sterowanie Systemem Sygnalizacji Pożaru oraz mieć możliwość sterownia wszystkimi urządzeniami pożarowymi indywidualnie oraz strefowo (zatrzymanie scenariusza na wypadek wystąpienia pożaru w danej strefie i uruchomienia w (dla) innej )
* Powinien posiadać plany w formacie DWG, SVG oraz HTML z rozbudowaną nawigacją po planach poprzez zastosowanie funkcji scrolla myszki komputerowej, z możliwością przeciągania planu w równych kierunkach przy dokonanym zoomie, z dostępnymi funkcjami z poziomu prawego klawisza myszki komputerowej.
* Czujniki na planie powinny być wyświetlane warstwowo dla poszczególnych systemów
* z możliwością wygaszania warstw i zdefiniowanych widoków (wycinków) na wypadek zdarzenia z danego systemu.
* System powinien posiadać możliwość tworzenia raportów dziennych, miesięcznych, kwartalnych ze sprawności integrowanych systemów.
* System powinien posiadać możliwość wykonywania okresowych testów instalacji pożarowej.
* System powinien mieć wbudowane narzędzia do wyświetlania oraz analizy mierzonych wartości.
* System powinien posiadać możliwość tworzenia indywidualnych procedur działania na wypadek zdarzenia w budynku z możliwością rozgałęzienia procedur na kolejne etapy
* w zależność od działań podjętych przez operatora.
* System powinien posiadać możliwość załączania dowolnych dokumentów takich jak karty katalogowe, instrukcje, przypisanych do konkretnych procedur działania, czujników lub urządzeń,
* System powinien mieć możliwość podłączenia dowolnego za pomocą protokołu komunikacyjnego.
* System powinien umożliwić podłączanie dowolnych urządzeń komunikujących się za pomocą styku (sterowanie i nadzorowanie – w tym urządzenia ochrony przeciwpożarowej)
* System powinien mieć możliwość tworzenia indywidualnych stanowisk obsługi dla poszczególnych budynków jak i możliwość nadzorowania wszystkich budynków z jednej stacji operatorskiej.
* Należy zapewnić bezpieczne połączenie z serwerem za pomocą SSL,
* System musi umożliwiać filtrowanie aktywnych alarmów dla dowolnego zdarzenia,
* System musi pracować w architekturze zorientowanej na usługi (ang. SOA)
* Wymagany jest mechanizm automatycznego wykonywania kopii zapasowych zgodnie z harmonogramem, na żądanie i z podziałem na kopiowane fragmenty systemu takie jak baza danych, logi, usługi, pliki konfiguracyjne, dokumentacje, instrukcje, zagnieżdżone elementu.
* System musi zapewnić możliwość implementacji instrukcji bezpieczeństwa pożarowego,
* PSIM musi posiadać moduł wprowadzania adresów i kontaktów - baza serwisantów, pojazdów itp.
* Ma mieć możliwość obsługi w języku min. polskim, niemieckim, angielskim.

**Wymagania formalno-prawne:**

* Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. 1997 Nr 114, poz. 740);
* Ustawa z dn. 7.07.1994 Prawo budowlane (Dz. U. 1994 Nr 89 poz. 414)
* Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2002 r. Nr 147, poz. 1229 z późn. zm.);
* Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie wraz z późniejszymi zmianami.
* Obwieszczenie Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 28 sierpnia 2003 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Pracy i Polityki Socjalnej w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (Dz.U. 2003 nr 169 poz. 1650) wraz ze zmianami.
* Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7.06.2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. z 2010 nr 109, poz. 719).
* Narodowy Program Ochrony Infrastruktury Krytycznej.
* Norma PN-EN 50131-1:2009 „Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe” lub równoważna;
* Zmiana do Polskiej Normy PN-EN 50131-1:2009/A1 sierpień 2010
* Norma PN-EN 62676-4 „Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 4: Wytyczne stosowania” lub równoważna;
* Norma PN-EN 60839-11-1:2014-01/AC „Systemy alarmowe i elektroniczne systemy zabezpieczeń Część 11-1: Elektroniczne systemy kontroli dostępu. Wymagania dotyczące systemów i części składowych” lub równoważna
* PKN-CEN/TS 54-14. Systemy sygnalizacji pożarowej Część 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji
* PN-EN 50173-1:2018-07 „Technika Informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne” lub równoważna
* PN-EN 50173-2:2018-07 „Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Budynki biurowe” lub równoważna
* PN-EN 50173-6:2018-07 „Technika Informatyczna – Systemy okablowania strukturalnego – Część 6: Rozproszone usługi budynkowe” lub równoważna
* PN-EN 50174-1:2018-08 „Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja instalacji i zapewnienie jakości” lub równoważna
* PN-EN 50174-2:2018-08 „Technika informatyczna. Instalacja okablowania – Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków lub równoważna
* PN-EN 50174-3:2014-02/A1:2017-07 „Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków” lub równoważna
* Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, z późniejszymi zmianami.
* Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, z późniejszymi zmianami.
* Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, z późniejszymi zmianami.
* Ustawa z dnia 5 lipca 20218 r. o krajowym systemie cyberbezpieczeństwa, z późniejszymi zmianami.
* Rozporządzeniem Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.
* Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych.
* Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne.
* Normą PN-EN 50130-4:2012 Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów sygnalizacji pożarowej, sygnalizacji włamania, sygnalizacji napadu, CCTV, kontroli dostępu i osobistych.
* Norma PN-EN 50130-5:2012 Systemy alarmowe – Część 5: Próby środowiskowe.
* Grupą Norm PN-EN 50136: Systemy alarmowe. Systemy i urządzenia transmisji alarmu.
* Grupą Norm PN-EN 50398: Systemy alarmowe. Systemy alarmowe łączone i zintegrowane.
* Grupa Norm PN-EN 50518: Centrum monitoringu i odbioru alarmu.
* Normą PN-EN 50346:2004/A2:2010 Technika informatyczna - Instalacja okablowania - Badanie zainstalowanego okablowania.
* Norma PN-EN ISO/IEC 27000:2017-06 Technika informatyczna - Techniki bezpieczeństwa -Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia.
* Normą PN-EN ISO/IEC 27001:2017-06 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagani.
* Normą PN-ISO/IEC 20000-1:2014-01 Technika informatyczna - Zarządzanie usługami.
* ISO/IEC 11801-1:2017 Information technology - Generic cabling for customer premises.
* Normą N-SEP-E-007:2017-09 Instalacje elektroenergetyczne i teletechniczne w budynkach – dobór kabli i innych przewodów ze względu na ich reakcję na ogień.
* Normą PN-EN 61082-1: Przygotowanie dokumentów stosowanych w elektrotechnice. Wymagania ogólne.
* Normą PN-82/E-01246: Rysunek techniczny elektryczny. Zasady wykonania schematów i  planów.
* Innymi aktami prawnymi i normatywnymi mającymi zastosowanie w zakresie   
  Przedmiotu Zamówienia.
* Zasadami sztuki, dobrych praktyk i aktualną wiedzą techniczną.
* Wymaganiami Zamawiającego opisanymi w Opisie Przedmiotu Zamówienia oraz dokumentacji postępowania.

**Wykaz oświadczeń i dokumentów, jakie mają dostarczyć wykonawcy w celu potwierdzenia posiadania wymaganej wiedzy i doświadczenia**

1. Wykonawca potwierdza, że dysponuje personelem posiadającymi niezbędne kwalifikacje do realizacji wdrożenia przedmiotu zamówienia, oraz że osoby wykonujące prace będą posiadały wszelkie bezwzględnie wymagane przepisami prawa uprawnienia. Przed przystąpieniem do wykonywania prac Wykonawca przedłoży Zamawiającemu listę osób posiadających stosowne uprawnienia.
2. Wykonawca musi posiadać koncesję MSWiA na świadczenie usług ochrony osób i mienia w formie zabezpieczeń technicznych.
3. Wykonawca zobowiązany jest spełnić wymagania Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych w zakresie informacji oznaczonych klauzulą co najmniej „Zastrzeżone”.
4. Osoby skierowane do realizacji Przedmiotu Zamówienia (od Etapu - dokumentacja powykonawcza) muszą posiadać dostęp do informacji niejawnych o klauzuli co najmniej „Zastrzeżone”.
5. Wykonawca skieruje do wykonania przedmiotu umowy jedynie osoby posiadające ukończone branżowe kursy i szkolenia potwierdzone zaświadczeniami, w szczególności:
6. wpis na listę kwalifikowanych pracowników zabezpieczenia technicznego – każda osoba prowadząca prace instalacyjne na obiekcie i uczestnicząca przy opracowaniu dokumentacji wykonawczej/powykonawczej;
7. uprawnienia do projektowania systemów zabezpieczeń technicznych stopni 1-4 – przynajmniej jedna osoba wykonująca projekt wykonawczy i dokumentację powykonawczą w zakresie przedmiotu zamówienia;
8. świadectwo kwalifikacyjne elektrycznej do 1kV na stanowisku dozoru zgodnie z przepisami rozporządzenia Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 28 kwietnia 2003r. w sprawie szczegółowych zasad stwierdzenia posiadania kwalifikacji przez osoby zajmujące się eksploatacją urządzeń, instalacji i sieci – przynajmniej jedna osoba prowadząca prace na obiektach;
9. świadectwo kwalifikacyjne elektrycznej do 1kV na stanowisku eksploatacji zgodnie z przepisami rozporządzenia Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 28 kwietnia 2003r. w sprawie szczegółowych zasad stwierdzenia posiadania kwalifikacji przez osoby zajmujące się eksploatacją urządzeń, instalacji i sieci – każda osoba prowadząca prace instalacyjne;
10. uprawnienia budowlane do projektowania bez ograniczeń w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń telekomunikacyjnych – przynajmniej jedna osoba wykonująca projekt wykonawczy i dokumentację powykonawczą Systemów;
11. uprawnienia budowlane do projektowania bez ograniczeń w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych – przynajmniej jedna osoba wykonująca dokumentacje projektową i powykonawczą Systemów;
12. certyfikat ukończenia kursów/szkoleń branżowych w zakresie instalacji i konfiguracji proponowanego systemu potwierdzony przez producenta lub autoryzowanego dystrybutora – przynajmniej cztery osoby prowadzące prace na obiektach;
13. certyfikat ukończenia kursów/szkoleń branżowych w zakresie konserwacji i serwisu proponowanego systemu potwierdzony przez producenta lub autoryzowanego dystrybutora – każda osoba prowadząca prace konserwacyjne i serwisowe na obiektach;
14. certyfikat ukończenia kursów/szkoleń branżowych w zakresie projektowania proponowanego systemu potwierdzony przez producenta lub autoryzowanego dystrybutora – przynajmniej jedna osoba wykonująca projekt wykonawczy i dokumentację powykonawczą Systemu;
15. Wykonawca zobowiązany jest do przestrzegania przepisów w zakresie BHP, Ppoż. i OŚ oraz wewnętrznych uregulowań i wymagań obowiązujących w organizacji Zamawiającego;
16. Wykonawca (jeżeli nie jest producentem proponowanego Systemu) musi załączyć oświadczenie producenta, iż jest certyfikowanym partnerem, dystrybutorem lub rekomendowanym integratorem dostarczanych rozwiązań.