Minimalne wymagania dla systemów bezpieczeństwa przeznaczonych do zainstalowania na EW Koronowo i EW Smukała.

1. Minimalne wymagania dla Systemu CCTV

Serwer zarządzania i rejestracji

- Do zarządzania i rejestracji obrazu z kamer w systemie wymaga się wykorzystanie dedykowanego rozwiązania serwerowego, łączącego w sobie funkcje serwera zarządzającego i przestrzeni dyskowej do zapisu, zgodnego z już wdrożonym rozwiązaniem.
- Urządzenie jest przeznaczone do bezpośredniego montażu w szafie rack.
- Serwer zarządzający ma być dostarczony od producenta w formie prekonfigurowanej, z gotowym do użycia oprogramowaniem zarządzającym.
- Pojedynczy serwer umożliwi podłączenie, zarządzanie i rejestrację do 256 kamer (kanałów wideo) w systemie.
- Serwer oraz oprogramowania zarządzania wideo umożliwi jednoczesne podłączenie do 10, w pełni funkcjonalnych stacji klienckich.
- Serwer ma być wyposażony w dwa wydajne i redundantne zasilacze, pracujące w trybie „hot-swap".
- Serwer ma być wyposażony w dyski SATA-3 do rejestracji, do których zapewniony jest dostęp od frontu urządzenia, umożliwiając łatwą wymianę dysków.
- Serwer ma posiadać wbudowany transkoder, umożliwiający wykorzystanie technologii transkodowania dynamicznego, dopasowującego parametry strumienia wizyjnego, przekazywanego do aplikacji klienckich, do aktualnych możliwości łącza.
- Serwer zarządzający ma wspierać technologie SNMP, zdalnego pulpitu czy monitorowania http elementów sprzętowych i aplikacji zarządzającej.

System zarządzania wideo VMS

- System zarządzający umożliwi obsługę kamer i enkoderów, realizujących funkcję rejestracji bezpośrednio przez urządzenie końcowe, w celu bezpośredniej rejestracji strumienia wideo z kamery na przestrzeni dyskowej iSCSI.
- System zarządzający nie będzie odpowiedzialny w takim przypadku za przetwarzanie strumienia czy rejestrowanych danych.
- System zarządzania umożliwi jednoczesne zarządzanie wieloma urządzeniami rejestrującymi.
- Przestrzenie dyskowe oraz opcje zapisu w razie usterki mogą być konfigurowane z poziomu konfiguratora oprogramowania zarządzającego.
- System zarządzający umożliwi rejestrację kamer zgodnych z ONVIF Profile S za pośrednictwem rejestratora serwerowego, zapisującego nagrania na przestrzeni dyskowej iSCSI.
- System umożliwi zarządzanie wszystkimi dostępnymi macierzami dyskowymi w konfiguracji pojedynczej puli lub wielu dostępnych puli zapisu.
- Przestrzeń dyskowa, w obrębie dostępnej puli zapisu, będzie przypisywana w sposób dynamiczny podłączonym kamerom, enkoderom, czy rejestratorom. Nie zachodzi przy tym potrzeba stałego przypisania kamer czy enkoderów do wybranej i określonej macierzy dyskowej. Dzięki temu zagwarantowane jest optymalne wykorzystanie dostępnej przestrzeni, jak również równomierne obciążenie sieci i urządzeń.

- Transfer danych z enkoderów, kamer i rejestratorów jest kontrolowany w oparciu o dostępną przepustowość łącza sieciowego oraz wydajność danej macierzy dyskowej.
- W razie trwałej usterki kamery, zapisane nagrania mogą być przypisane ponownie do podłączonego, nowego urządzenia.
- W przypadku nagrywania alarmowego, buforowanie fragmentu nagrań przed wystąpieniem alarmu może odbywać się w kamerze IP, wyposażonej w pamięć podręczną, a fragment ten zostanie zapisany na macierzy dyskowej jedynie po wystąpieniu alarmu, aby ograniczyć obciążenie sieci.
- Możliwe jest skonfigurowanie do 7 rodzajów rejestracji przed wystąpieniem alarmu dla każdej kamery IP, w zależności od różnych zdarzeń lub zdarzeń złożonych.
- System rejestracji ma obsługiwać urządzenia, umożliwiające bezpośrednią rejestrację, z wykorzystaniem protokołu iSCSI.
- Kamery, wykorzystujące funkcję samodzielnej rejestracji na przestrzeni dyskowej, mają samodzielnie rejestrować nagrania na macierzy, bez pośrednictwa serwera czy dodatkowego rejestratora.
- Kamery mają wykorzystywać mechanizm lokalnego buforowania, umożliwiający redukcję wpływu krótkotrwałych przerw w transmisji sieciowej i rejestrację bez utraty fragmentów nagrań.
- System zarządzania wideo umożliwi pełną obsługę kodowania h.264 oraz h.265.
- System zarządzania wideo umożliwi konfigurację alarmu, gdy dojdzie do ręcznego usunięcia zarejestrowanych nagrań wideo.

Skalowalność

- System będzie wchodził w skład większego systemu rozproszonego, dla którego pojedynczy serwer zarządzający staje się niezależnym, w pełni autonomicznym podsystemem.

Niezawodność i odporność na awarie

- System zarządzania wideo ma mieć możliwość wsparcia funkcji automatycznego buforowania lokalnie w razie usterki połączenia sieciowego
    - Nagrania są buforowane w pamięci (karcie SD) kamery IP w razie braku komunikacji sieciowej. System zarządzania umożliwia alarmowanie, gdy kończy się dostępna przestrzeń rejestracji lub nagrania są usuwane z racji niewystarczającej przestrzeni dyskowej. Po przywróceniu komunikacji sieciowej, kamera automatycznie uzupełnia nagrania na macierzy dyskowej. Proces ten powinien odbywać się automatycznie i nie wymaga udziału użytkownika.
- Aplikacja kliencka ma wskazywać status połączenia z serwerem zarządzającym.
    - Aplikacja kliencka ma pracować dalej również, gdy serwer zarządzający jest niedostępny,
    - Informowanie o statusie połączenia ma obejmować stan połączony, rozłączony, czy brak synchronizacji konfiguracji aplikacji klienckiej względem serwera zarządzającego,
    - Status połączenia z serwerem zarządzającym ma być wskazany przy ikonie na liście urządzeń
- System ma być wykonany w taki sposób, aby zmiany konfiguracji dowolnej części systemu nie zaburzały obsługi, zanim operator nie zdecyduje się na aktualizację i odświeżenie konfiguracji stacji roboczej.

- System zarządzania wideo ma cechować się wysokim stopniem odporności na awarie. Nawet w przypadku jednoczesnej usterki serwerów zarządzających oraz macierzy dyskowych, operatorzy powinni wciąż mieć możliwość podglądu obrazu z kamer i sterowania nimi, jak również odtwarzania nagrań z karty pamięci w kamerze lub innej formy rejestracji w razie awarii.
    - Niedostępność serwera zarządzającego nie może wpływać na stan rejestracji obrazu z kamer – jeśli dostępna jest przestrzeń dyskowa do zapisu.
    - Po ponownym uruchomieniu/podłączeniu brakujących komponentów systemu, nie jest wymagane żadne działanie użytkownika czy administratora w celu powrotu do normalnego trybu pracy systemu.
- Operator ma mieć możliwość uruchomienia aplikacji klienckiej nawet, gdy serwer zarządzający jest niedostępny.
- System zarządzania wideo ma gwarantować, że alarmy zostaną zapamiętane również po poprawnym, ponownym uruchomieniu serwera zarządzającego.

Oprogramowanie klienckie

- Stacje robocze systemu zarządzania wideo mają umożliwiać podłączenie do 4 monitorów, a każdy z monitorów może być niezależnie skonfigurowany do wyświetlania obrazu z kamer na żywo, odtwarzania nagrań, map lokalizacji lub zdarzeń alarmowych.
- Aplikacja kliencka systemu zarządzania wideo udostępni interfejs użytkownika do monitorowania i obsługi systemu. Aplikacja kliencka umożliwi podgląd na żywo, przeglądanie i pobieranie nagrań oraz obsługę alarmów.
- Użytkownik ma mieć możliwość przeszukiwania drzewa logicznego w poszukiwaniu nazw elementów systemu (na przykład kamery).
- System zarządzania wideo zaoferuje każdemu z użytkowników niezależną listę zakładek
    - Lista zakładek umożliwi zapisanie zakresu czasowego lub określonego punktu w czasie dla późniejszej analizy i eksportu
    - Zakładki powinny być dostępne zarówno w trybie na żywo, jak i w trybie odtwarzania.
- System zarządzania wideo zaoferuje każdemu z użytkowników niezależną listę ulubionych
    - Drzewo ulubionych ma umożliwiać skonfigurowanie map, folderów i urządzeń oraz pełnych widoków (układ okien wideo z przypisanymi kamerami) przez każdego użytkownika w strukturze zdefiniowanej przez użytkownika,
    - Drzewo ulubionych użytkownika ma być dostępne niezależnie od komputera, na którym loguje się on do systemu,
    - Możliwe ma być dostosowanie różnych widoków dla każdego okienka obrazu za pomocą funkcji
    - e-PTZ i zapisanie tak stworzonych widoków jako ulubiony
    - Podczas wybierania ulubionych na ekranie wyświetli się spersonalizowany podgląd na żywo tej samej kamery (kamer).
- System zarządzania wideo ma zawierać okno, które wyświetla zbiór okienek z podglądem. Układ musi zapewniać optymalizację zarówno dla monitorów standardowych (4:3), jak i panoramicznych (16:9).

  - W przypadku standardowych monitorów liczba okienek z podglądem na okno będzie się zmieniać w zakresie od 1 (pojedynczego wideo w pełnym oknie) do 25, ułożonych w siatkę 5x5. Dostępny musi być suwak pozwalający na zmianę rozmiaru siatki w zakresie 1x1, 2x2, 3x3, 4x4 i 5x5.
  - W przypadku monitorów szerokoekranowych liczba okienek z podglądem na okno może się zmieniać w zakresie od 1 do 30, ułożonych w siatkę 1x1, 3x2, 4x3, 5x4 i 6x5.
  - Liczba okienek z podglądem, dostępnych dla operatora, może być ograniczona w zależności od konfiguracji danej grupy użytkowników.
  - System zarządzania wideo ma umożliwiać powiększanie lub zmniejszanie paneli obrazu w obrębie siatki. Przykładowo, w siatce 5x5 pojedynczy panel obrazu można powiększyć, aby wykorzystać cztery okienka podstawowe siatki, tworząc większe okno podglądu. Pozwala to operatorowi oglądać wideo w dowolnym wzorze utworzonym w strukturze siatki.
  - Operator nie będzie ograniczony jedynie do wstępnie skonfigurowanych układów, ale powinien mieć również możliwość zmiany rozmiaru okna podglądu, klikając i przeciągając krawędź okienka obrazu, aby przeciągnąć granicę w poziomie lub w pionie lub klikając róg okienka obrazu, aby przeciągnąć róg okienka po przekątnej, do żądanego rozmiaru.
  - Aplikacja kliencka ma umożliwiać wybranie i podświetlenie danego okienka podglądu.
- Jedno z okienek podglądu aplikacji klienckiej ma pozostawać wybrane i podświetlone
- Wybrane i podświetlone okienko podglądu jest zawsze używane dla poleceń sterujących, np. natychmiastowego sterowania PTZ, sterowania odtwarzaniem nagrań oraz odtwarzania dźwięku
- System zarządzania wideo będzie mieć możliwość obsługi źródła dźwięku dla podłączonych kamer IP oraz enkoderów. Powinno być możliwe przypisanie źródeł audio do kamer.
  - Aplikacja kliencka umożliwi włączenie/wyłączenie odtwarzania dźwięku dla każdej kamery.
  - System zarządzania wideo ma wspierać dwa różne tryby audio – jednoźródłowe oraz wieloźródłowe.
- W trybie jednoźródłowym ma mieć możliwość odtwarzania jedynie dźwięk dla źródła, przypisanego do kamery w aktualnie wybranym okienku podglądu,
- W trybie wieloźródłowym ma mieć możliwość odtwarzania dźwięku dla wszystkich źródeł audio kamer, wyświetlanych w aplikacji klienckiej
- Aplikacja kliencka systemu zarządzania wideo umożliwi korygowanie odkształceń i tworzenie widoków panoramicznych dla kamer 360^{o}, zarówno przy podglądzie na żywo, jak i w trakcie odtwarzania nagrań.
- Aplikacja kliencka umożliwi opcjonalnie wyświetlenie informacji z funkcji inteligentnej analizy obrazu w kamerze, takich jak obszary detekcji ruchu, maski obiektu oraz trajektorie, zarówno przy podglądzie na żywo, jak i w trakcie odtwarzania nagrań.
- System zarządzania wideo będzie w sposób graficzny wskazywał stany urządzeń przy ich ikonach na liście lub na mapie.
  - W przypadku kamer, wyświetlane będą informacje o następujących stanach: utrata sygnału wideo, utrata połączenia sieciowego, rejestrowanie nagrań, zakłócenia obrazu wideo, prześwietlenie obrazu, obraz zbyt ciemny, brak kalibracji obrazu oraz sygnał audio przypisany dla strumienia wideo

  - Dla przekaźników oraz wejść stykowych, wskazywany jest stan otwarcia lub zamknięcia.
- Aplikacja kliencka umożliwi zagnieżdżenie i otwarcie w oknie aplikacji dla systemu Windows, dając operatorowi możliwość otwarcia wielu aplikacji w jednym oknie interfejsu systemu zarządzania wideo.
- Aplikacja kliencka ma umożliwiać sterowanie kamerami typu PTZ z wykorzystaniem:
  - Graficznego elementu sterującego („joystick'a") do kontrolowania kąta obrotu, pochylenia, przybliżenia, przesłony, wyostrzenia oraz poleceń pomocniczych
  - Kliknięcia i przeciągnięcia myszy wewnątrz okienka z podglądem obrazu
- W przypadku wybranych kamer typu PTZ, oferujących funkcję automatycznego podążania za wykrytym obiektem, aplikacja kliencka ma dawać możliwość uruchomienia tego typu funkcjonalności i śledzenia po kliknięciu na wybranym obiekcie w podglądzie na żywo.

Odtwarzanie i przeglądanie nagrań

- System zarządzania wideo przy przeglądaniu nagrań wyświetli linię czasu i w sposób graficzny przedstawi przegląd nagrań, zapisanych na dysku
  - Skala czasu umożliwi ustawienie podziałki od co najmniej 15 minut do co najmniej 1 miesiąca
  - Linia ma w sposób kolorystyczny wskazywać zakres czasu, dla którego dostępne są nagrania.
  - Nagrania zabezpieczone przed nadpisaniem lub usunięciem ma być oznaczone kreskowaniem
  - Przy linii powinno istnieć wskazanie informujące o dostępności strumienia audio, powiązanego z nagraniami w danym zakresie czasu
- System zarządzania wideo obsługuje przeszukiwanie nagrań pod kątem ruchu w określonych przez użytkownika obszarach obrazu z kamery.
- System zarządzania wideo ma wspierać przeszukiwanie nagrań co najmniej w oparciu o następujące kryteria: rozmiar obiektu, kolor obiektu, kierunek ruchu i prędkość oraz wykrycie obiektów wkraczających lub opuszczających wybrane obszary.
- System zarządzania ma umożliwiać przeszukiwanie nagrań na podstawie dowolnej kombinacji zakresu czasu/daty, rodzaju zdarzenia, priorytetu alarmu, stanu alarmowego oraz urządzenia (urządzeń).
- Ma mieć możliwość zapisania i przywrócenia parametrów wyszukiwania
- System zarządzania umożliwi wyszukiwanie danych tekstowych, przechwyconych z urządzeń typu bankomat, kasa, czytnik kodów kreskowych i innych. Ma mieć możliwość przeszukiwania bazy danych w oparciu o fragment tekstu i znaki zastępcze
- Wyniki wyszukiwania są prezentowane w postaci listy a wybór danego wyniku powoduje bezpośrednie wyświetlenie nagrań zarejestrowanych w danym momencie wraz z danymi tekstowymi.
- Dane tekstowe są wyświetlane w oknie podglądu danej, odtwarzanej kamery. Możliwe jest zatem jednoczesne wyświetlenie danych tekstowych dla wielu kamer.
- Operator powinien mieć możliwość wyboru czy dane tekstowe powinny być wyświetlane po prawej stronie czy pod oknem podglądu.

Wydajność

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

Obsługa map

- System zarządzający umożliwi tworzenie map lokalizacji z aktywnymi ikonami dla urządzeń (kamer, przekaźników sterujących, wejść przekaźnikowych i innych elementów systemu), uruchamiania poleceń dla skryptów, uruchamiania sekwencji kamer i z linkami do innych map lokalizacji.
- Ma być możliwe przybliżanie i oddalanie map dla wygodnej pracy z systemem.
- Aktywne ikony umożliwią takie skonfigurowanie, aby wyświetlona została nazwa urządzenia lub nazwa linku.
- Status danego urządzenia ma być przedstawiony w sposób graficzny przy odpowiedniej ikonie na mapie.
- Ma być możliwe skonfigurowanie priorytetów zdarzeń dla urządzeń tak, aby wizualizowane było tylko jedno zdarzenie dla danej ikony na mapie w momencie jednoczesnego wystąpienia wielu zdarzeń.
- Po najechaniu kursorem myszy na ikonę na mapie aplikacja ma wyświetlić podgląd widoku z danej kamery, dla łatwiej identyfikacji urządzenia.
- Menu kontekstowe, przypisane do ikony kamery typu PTZ na mapie, umożliwi wybranie określonych położeń zaprogramowanych.
- Ma być możliwe zaakceptowanie i usunięcie alarmu z danej kamery, korzystając z menu kontekstowego danej ikony na mapie.

Zarządzanie alarmami

- System zarządzania wideo umożliwi tworzenie alarmów zależnych od harmonogramu.
- System umożliwi przypisanie poszczególnych alarmów do określonych grup użytkowników.
- System umożliwi replikację zdarzeń w taki sposób, że jedno zdarzenie fizyczne w systemie generuje liczne zdarzenia systemowe. Takie zdarzenie można niezależnie

skonfigurować, by umożliwić niezależną obsługę alarmów różnym grupom operatorów lub w sposób zależny od harmonogramu czasowego.

- System zarządzania ma umożliwiać zaprogramowanie alarmów tak, aby w sposób selektywny, w zależności od stanu alarmowego lub grupy użytkowników, automatycznie wyświetlić obraz z kamery powiązanej ze zdarzeniem.
- Okno alarmowe systemu umożliwi takie skonfigurowanie, by wyświetlony został podgląd na żywo, odtwarzanie nagrań, dokumenty tekstowe, mapy obiektów, pliki HTML lub witryny (adresy URL). Dla każdego alarmu możliwe jest skonfigurowanie jednego okna odtwarzania nagrań i jednej mapy.
- System ma oferować reakcję na alarm w czasie maksymalnie 2 sekund, gdy dostępna jest wystarczająca przepustowość sieci.
- System umożliwi dystrybuowanie powiadomień o alarmach, poprzez wpisy na liście alarmowej interfejsu operatora, do wszystkich członków określonej grupy użytkowników.
- Gdy alarm zostanie zaakceptowany przez danego użytkownika, ma zostać usunięty z listy alarmowej innych użytkowników grupy
- System umożliwi wycofanie potwierdzenia alarmu. W takim przypadku alarm pojawi się ponownie na liście alarmowej wszystkich członków grupy użytkowników, do której przypisany został alarm.
- System umożliwi wysłanie wiadomości e-mail lub SMS w odpowiedzi na alarm.

Wykorzystanie skryptów

- System zarządzania wideo ma oferować wbudowany edytor skryptów poleceń, umożliwiający napisanie własnych skryptów do wirtualnego sterowania funkcjami systemu. Skrypty poleceń mogą być uruchamiane przez operatorów lub automatycznie, w odpowiedzi na zdarzenia alarmowe lub systemowe. Wbudowany edytor skryptów poleceń wspiera języki C# oraz VB.NET.
- System ma być konfigurowalny w taki sposób, że operatorzy mogą wykonywać stworzone skrypty przez podwójne kliknięcie na odpowiednich ikonach w drzewie logicznym lub na mapie lokalizacji.
- System umożliwi konfigurację w taki sposób, że stworzone skrypty są wykonywane automatycznie w odpowiedzi na zdarzenia systemowe. Automatyczne wykonywanie skryptów może być opcjonalnie ograniczone harmonogramami.
- System umożliwi wykonanie skryptów poleceń dla danej grupy użytkowników w momencie zalogowania użytkownika do systemu.
- System umożliwi wykonanie skryptów poleceń dla alarmów w momencie zaakceptowania alarmu przez operatora

Infrastruktura IT

- Podgląd obrazu z kamer ma być możliwy na jednej lub wielu stacjach roboczych jednocześnie. Kamery, rejestratory i stacje robocze mogą być umieszczone w dowolnym miejscu w sieci IP.
- Aktualizacje programowe aplikacji klienckich oraz oprogramowania konfiguracyjnego muszą być automatycznie i centralnie wdrażane przez serwer zarządzający.

- System zarządzania ma wspierać protokół LDAP, umożliwiający integrację z systemami zarządzania użytkownikami, jak Microsoft Active Directory.
- Oprogramowanie serwera zarządzającego umożliwi zarządzanie, monitorowanie i kontrolę pracy całego systemu.
- System zarządzania umożliwi monitorowanie urządzeń poprzez protokół SNMP (co najmniej SMNPv2).

Integracja z systemami zewnętrznymi

- System zarządzania wideo umożliwi integrację z:
  - Systemami rozpoznawania twarzy
  - Naziemnymi systemami detekcji radarowej
  - Systemami ochrony perymetrycznej
  - Systemami zarządzania bezpieczeństwem fizycznym
  - Systemami rozpoznawania tablic rejestracyjnych
- System zarządzania wideo ma umożliwiać uruchomienie zdarzenia alarmowego, na podstawie informacji otrzymanej z tego typu systemów.
- System zarządzania wideo umożliwi modyfikację, z wykorzystaniem SDK, tak, aby:
  - weryfikować alarm z innych systemów (baz danych) przed zaprezentowaniem operatorowi.
  - przesłać informacje do innych systemów z wykorzystaniem dedykowanych protokołów.
- Dla systemu zarządzania wideo dostępne są udokumentowane biblioteki SDK (Software Development Kit), umożliwiające integracje z oprogramowaniem firm trzecich.
- Funkcjonalności SDK wymaga autentykacji w systemie.
- Biblioteki SDK mają być dostępne dla wszystkich języków programowania .Net.
- System zarządzania wideo ma posiadać wbudowany serwer OPC do integracji z oprogramowaniem zewnętrznym, takim jak systemy BMS, SMS, czy PSIM.
- Interfejs OPC ma obsługiwać standard OPC Alarms and Events.

Obsługa inteligentnej analizy obrazu

- System zarządzania wideo umożliwi konfigurację parametrów inteligentnej analizy obrazu w urządzeniu końcowym z poziomu interfejsu konfiguracyjnego.
- System będzie reagował na zdarzenia, wywołane funkcjami inteligentnej analizy obrazu w urządzeniu końcowym, w tym w kamerze IP lub enkoderze.
- Wszystkie zdarzenia mają być zapisywane w dzienniku zdarzeń, umożliwiając późniejsze przeszukiwanie.
- Metadane, generowane przez urządzenia końcowe, mają być zapisywane wraz z nagraniami, co umożliwia operatorowi szybkie przeszukiwanie nagrań pod kątem określonych zdarzeń również wtedy, gdy alarmy inteligentnej analizy obrazu nie zostały uprzednio skonfigurowane w kamerze.
- Aplikacja kliencka umożliwi operatorowi podgląd reguł alarmowych, skonfigurowanych w kamerach z funkcją inteligentnej analizy obrazu.

Bezpieczeństwo systemu

- System zarządzania wideo umożliwi stworzenie grup użytkowników z uprawnieniami do dostępu do określonych kamer, priorytetem sterowania PTZ, uprawnieniami

eksportowania nagrań oraz dostępu do dziennika zdarzeń systemowych. Dostęp do podglądu na żywo, nagrań wideo, audio, sterowania PTZ, wywoływania położeń zaprogramowanych i poleceń pomocniczych może być programowany na poziomie pojedynczej kamery w systemie.

- Aby ograniczyć potencjalne ryzyko ataku typu „brute-force", system nie może posiadać niemodyfikowalnego konta o uprawnieniach administratora.
- System zarządzania umożliwi stworzenie grup użytkowników, gdzie wymagane jest uwierzytelnianie dwupoziomowe.
- System zarządzania wideo umożliwi potwierdzenie autentyczności zarejestrowanych nagrań. Wspierane ma być sprawdzenie wartości sumy kontrolnej względem danych wideo z kamer, które dostarczają strumień do rejestracji z wartościami sumy kontrolnej, podpisanymi certyfikatem.
- Oprogramowanie klienckie umożliwi wylogowanie bezpieczeństwa po upływie określonego czasu bezczynności
  - Aplikacja kliencka zostanie wylogowana automatycznie, gdy przez dany okres czasu nie zostanie wykryta aktywność operatora
- Ma być możliwe wymuszenie polityki bezpieczeństwa haseł logowania do aplikacji klienckiej przez użytkowników.
  - Gdy uruchomione zostanie wymuszenie ustanowienia bezpiecznego hasła, aplikacja kliencka będzie akceptować jedynie hasła:
- o długości co najmniej 8 znaków
- z przynajmniej jedną literą małą
- z przynajmniej jedną literą wielką
- Ma być możliwe zablokowanie konta po określonej, konfigurowalnej liczbie nieudanych prób logowania.
- Ma być możliwe skonfigurowanie maksymalnego czasu obowiązywania hasła.
- Ma być możliwa dezaktywacja konta użytkownika.
- Ma być możliwe wymuszenie zmiany hasła użytkownika przy kolejnym logowaniu.
- System zarządzania wideo umożliwi stworzenie grup użytkowników, mających uprawnienia dostępu do poszczególnych funkcji konfiguracyjnych, z podziałem na co najmniej: urządzenia, mapy i drzewo logiczne, harmonogramy, parametry rejestracji, zdarzenia, alarmy i grupy użytkowników.
- System zarządzania umożliwi skonfigurowanie danych uwierzytelniających dostęp do zewnętrznych zasobów sieciowych (aplikacji zagnieżdżonych), aby nie zachodziła potrzeba ręcznego logowania do tych zasobów przez operatora.
- Ma być możliwe skonfigurowanie bezpiecznej, szyfrowanej komunikacji pomiędzy serwerem zarządzającym a kamerami oraz pomiędzy aplikacją kliencką a kamerami
  - Aplikacja kliencka umożliwi dekodowanie obrazu z zabezpieczonego (AES-128) strumienia multicast
  - Aplikacja kliencka umożliwi dekodowanie obrazu z zabezpieczonego (AES-256) strumienia unicast
- System umożliwi szyfrowanie rejestrowanych danych poprzez AES-256 bez spadku wydajności (liczby obsługiwanych kamer i przepustowości) rejestratora.
- System zarządzający umożliwi odtwarzanie nagrań wideo, zaszyfrowanych poprzez AES-256.

Zapewnienie zgodności

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

Konfiguracja

- System zarządzania wideo ma oferować zintegrowany interfejs do konfiguracji i zarządzania systemem.
- System umożliwi skonfigurowanie domyślnie wyświetlanego strumienia z kamery względem określonej stacji roboczej i/lub względem danej kamery.
- Profile użytkowników, wraz z poszczególnymi ustawieniami mają być przechowywane centralnie, na serwerze. Ustawienia te mają być dostępne dla danego użytkownika niezależnie od fizycznej stacji roboczej, z której w danej chwili on korzysta.
- Zmiany, wprowadzane w konfiguracji systemu zarządzania wideo, będą wprowadzane w kopii roboczej aktualnej konfiguracji i nie będą bezpośrednio wpływały na aktywną i wykorzystywaną w danej chwili konfigurację systemu.
- Oprogramowanie konfiguracyjne umożliwi w dowolnym momencie aktywowanie kopii roboczej ustawień tak, aby stała się ona aktywną i wykorzystywaną konfiguracją systemu.
- Ma być możliwe ustalenie przyszłej daty i godziny, o której dana kopia konfiguracji stanie się aktywna.
- Aplikacja ma dawać operatorowi możliwość lokalnej aktywacji nowej konfiguracji natychmiast lub odłożenia tego procesu w czasie. Ma być możliwe również wymuszenie aktywacji nowej konfiguracji dla wszystkich aplikacji klienckich w obrębie danego serwera.
- System zarządzania wideo udostępni do 10 różnych i niezależnych harmonogramów nagrywania. Mogą one być wykorzystane do zapewnienia zmiennej liczby klatek na sekundę w ciągu dnia, nocy, czy dni wolnych i świątecznych. Harmonogramy mogą być również wykorzystane do umożliwienia logowania określonej grupie użytkowników, wyzwalania alarmów przez określone zdarzenia, czy eksportowania nagrań.

Rejestr zdarzeń

- System będzie zapisywał wszystkie zdarzenia i alarmy w bazie danych SQL. Wpis dotyczący alarmu zawiera nazwy kamer, dla których z racji wystąpienia danego alarmu zostało uruchomione nagrywanie.
- Rejestr zdarzeń umożliwi zapis co najmniej 500 000 zdarzeń na godzinę. W razie przekroczenia pojemności rejestru, usuwane będą najstarsze zapisy w bazie danych.

- Użytkownik ma mieć możliwość przeszukiwania rejestru pod kątem zdarzeń i alarmów. Wyniki mogą być wyeksportowane do zewnętrznego pliku CSV.
- System domyślnie ma być wyposażony w gotową do użycia bazę danych SQL. System opcjonalnie umożliwi wykorzystanie zewnętrznej instancji bazy danych SQL.
- System ma mieć możliwość konfiguracji czasu przechowywania zdarzeń w rejestrze.

Zgodność z normami

- Produkt musi pochodzić od firmy, spełniającej wymagania systemu zarządzania jakości ISO-9001 oraz EN-29001.
- System zarządzania wideo ma umożliwiać taką konfigurację, aby była możliwość zapewnienia zgodności z wymaganiami normy IEC 62676.
- System zarządzania wideo ma umożliwiać taką konfigurację, aby zapewniona została zgodność z wymaganiami RODO danej organizacji.

Wymagania dla kamery Bullet

Do dozoru przestrzeni zewnętrznych wymaga się wykorzystanie kamer zintegrowanych typu „bullet", o rozdzielczości 5MP. Dla zapewnienia wysokiej jakości obrazu również w ciemności, kamery mają posiadać wbudowany oświetlacz podczerwieni o zasięgu 50m. Kamera ma posiadać zintegrowany obiektyw z możliwością zdalnej regulacji ogniskowej, który daje możliwość łatwego dopasowania obserwowanej sceny oraz wyostrzenia obrazu z kamery.

Z racji dużej liczby kamer w systemie security, celem zachowania efektywności systemu bez znaczącego zwiększenia liczby operatorów przyjmuje się aktywne wykorzystanie mechanizmów zaawansowanej analizy obrazów dla kamer CCTV. Tym samym wszystkie kamery w systemie mają być fabrycznie wyposażone w funkcje inteligentnej analizy obrazu – nie wymaga to zakupu i uruchamiania dodatkowych licencji. Analiza obrazu ma odbywać się bezpośrednio w kamerze, dzięki czemu zapewniona jest najwyższa skuteczność (praca na nieskompresowanym obrazie) oraz skalowalność. Zakłada się wykorzystanie co najmniej następujących algorytmów analizy:

- Wykrywanie porzucenia przedmiotów
- Wejście w zastrzeżoną strefę
- Zliczanie obiektów
- Nienaturalne szwędanie się osób w wyznaczonych obszarach

W celu znacznie skuteczniejszego wykorzystania funkcji inteligentnej analizy obrazu, kamera ma być w stanie automatycznie sklasyfikować rozpoznany obiekt (jako człowieka, rowerzystę, czy samochód). Rodzaj obiektu będzie wskazany na obrazie poprzez wyświetlanie odpowiedniej ikonki, obok dokładnego obrysu obiektu.

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

Celem zwiększenia efektywności i skrócenia czasu przeszukiwania nagrań przez operatorów, algorytmy inteligentnej analizy obrazów mają być wykorzystywane również

do analizy wstecznej. Na podstawie metadanych zbieranych w systemie analityki, operator będzie w stanie szybko przeszukać zapisy pod kątem zdarzeń takich jak:

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

Istotną kwestią będzie także cyberbezpieczeństwo całego układu sieciowego i wszystkich systemów security bazujących na nim. Zakłada się szyfrowaną komunikację pomiędzy kamerami, serwerem zarządzającym, stacjami operatorskimi i systemem zapisu, przy wykorzystaniu algorytmów szyfrujących AES z kluczem 256 bit.

Kamera ma umożliwiać obsługę kart MicroSD o pojemności do 2 TB. W przypadku zastosowania kart w wykonaniu przemysłowym kamera ma mieć możliwość monitorowania aktualnego stanu karty i automatycznie alarmować, w przypadku przekroczenia określonego limitu jej żywotności.

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

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

Wymagania techniczne:

Kamera A

Parametr	**Wymagania minimalne**
Budowa	Kamera stałopozycyjna typu bullet z oświetlaczem IR
Rozdzielczość	3072 x 1728p30
Przetwornik	CMOS 1/ 2,9"
Czułość	Nie gorsza niż 0,37 lux w trybie dziennym i 0,035 lux w trybie nocnym dla obrazu 30IRE, reflektancji sceny 89%, F1.3. 0,0 lux przy włączonym oświetlaczu IR
Zakres dynamiki	120 dB
Kompresja	H.265, H.264, M-JPEG
Obszary ROI	Do 8 obszarów z niezależnymi ustawieniami jakości kodowania
Stosunek sygnał/szum	>55 dB
Migawka	Tryby migawki: automatyczna, wybierana ręcznie.
Oświetlacz IR	Wbudowany, o zasięgu 50 m, z regulacją intensywności
Obiektyw	Zintegrowany 2,7 - 12 mm ze zdalną regulacją zoom i autofocusem
Obsługiwane protokoły	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/ RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP, FTP, ARP, DHCP, APIPA (Auto-IP, link local address), NTP (SNTP), SNMP (V1, V3, MIB-II), 802.1x, DNS, DNSv6, DDNS, SMTP, iSCSI, UPnP (SSDP), DiffServ (QoS), LLDP, SOAP, Dropbox™, CHAP, digest authentication

Bezpieczeństwo danych	Wsparcie uwierzytelnienia poprzez protokół EAP-TLS 1.2 także z możliwością wgrania certyfikatu w zakresie infrastruktury klucza publicznego do szyfrowania cyfrowego dostarczonego przez producenta kamery, tworzonego przez użytkownika oraz certyfikowane rozwiązania firm 3-ch
	Wsparcie szyfrowania na poziomie sprzętowym tj fabrycznie zabudowany moduł TPM (Trusted Platform Module), który wykorzystuje klucz kryptograficzny do ochrony wszystkich zarejestrowanych danych
Autentykacja wideo	Znak wodny, SHA-1, SHA-256
Łącze sieciowe	RJ-45 100 Base-TX Ethernet
Strumienie wideo	Możliwość generowania 4 strumieni wideo
Inteligentna analiza obrazów	Wbudowana w kamerę z możliwością równoległej analizy do 8 reguł alarmowych
	Analizowane algorytmy: • wykrycie obiektu • przekroczenie linii • kierunkowość ruchu • porzucenie obiektu • zmiana stanu obiektu • zliczanie – przekroczenie linii • zliczanie obiektów w określonych strefach
	Zaawansowane funkcje w zakresie kalibracji i monitorowania obiektu takie jak np. ustalone proporcje obiektu, kolor obiektu oraz kierunek i prędkość jego przemieszczania
	Możliwość prezentowania statystyki dla wybranego pola lub obiektu z możliwością odczytu rzeczywistych wartości takich jak prędkości obiektu, jego proporcje i kolor czy kierunek jego poruszania
	Możliwość analizy materiału zarejestrowanego na podstawie metadanych
Zapis lokalny	Wbudowany slot karty SD/microSD (obsługa kart do 2 TB)
Pre-alarm	60s
Zgodność	ONVIF Profile S; ONVIF Profile G
Wejście alarmowe	1
Wyjście przekaźnikowe	1
Wejście audio	1
Wyjście audio	1
Alarm audio	Alarm na podstawie wykrycia dźwięku
Maski prywatności	8
Temperatura pracy	-40 - +60 st C
Zasilanie	Sieciowe lub PoE
Gwarancja	5 lat

Kamera B

Parametr	Wymagania minimalne
Budowa	Wytrzymała kamera typu bullet
Rozdzielczość	3840x2160 30p
Przetwornik	CMOS 1/1.8”
Obiektyw	3,7-10mm zmotoryzowany

Czułość	Nie gorsza niż 0,107 lux w trybie dziennym i 0,101 lux w trybie nocnym dla obrazu 30IRE, reflektancji sceny 89%, 0 lux przy włączonym oświetlaczu IR
Oświetlacz	40m
Stosunek sygnał/szum	>50 dB
Zakres dynamiki	108 dB
Kompresja	H.265, H.264, M-JPEG
Obsługiwane protokoły	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP, FTP, ARP, DHCP, APIPA (Auto-IP, link local address), NTP (SNTP), SNMP (V1, V3, MIB-II), 802.1x, DNS, DNSv6, DDNS (DynDNS.org, selfHOST.de, noip. com), SMTP, iSCSI, UPnP (SSDP), DiffServ (QoS), LLDP, SOAP, Dropbox™, CHAP, digest authentication
Bezpieczeństwo danych	Wsparcie uwierzytelnienia poprzez protokół EAP-TLS 1.2 także z możliwością wgrania certyfikatu w zakresie infrastruktury klucza publicznego do szyfrowania cyfrowego dostarczonego przez producenta kamery, tworzonego przez użytkownika oraz certyfikowane rozwiązania firm 3-ch
	Wsparcie szyfrowania na poziomie sprzętowym tj fabrycznie zabudowany moduł TPM (Trusted Platform Module), który wykorzystuje klucz kryptograficzny do ochrony wszystkich zarejestrowanych danych
Autentykacja wideo	Znak wodny, SHA-1, SHA-256
Łącze sieciowe	RJ-45 100 Base-TX Ethernet
Strumienie wideo	Możliwość generowania 3 strumieni wideo
Inteligentna analiza obrazów	Wbudowana w kamerę z możliwością równoległej analizy do 16 reguł alarmowych
	Analizowane algorytmy: • wykrycie obiektu • przekroczenie linii • kierunkowość ruchu • porzucenie obiektu • zmiana stanu obiektu • zliczanie – przekroczenie linii • zliczanie obiektów w określonych strefach
	Zaawansowane funkcje w zakresie kalibracji i monitorowania obiektu takie jak np. ustalone proporcje obiektu, kolor obiektu oraz kierunek i prędkość jego przemieszczania
	Możliwość prezentowania statystyki dla wybranego pola lub obiektu z możliwością odczytu rzeczywistych wartości takich jak prędkości obiektu, jego proporcje i kolor czy kierunek jego poruszania
	Możliwość analizy materiału zarejestrowanego na podstawie metadanych
Analiza obrazu – uczenie maszynowe	Możliwość stworzenie do 16 pól detekcji. Możliwość uczenia do 1000 próbek pozytywnych oraz 1000 próbek negatywnych.
Zgodność	ONVIF Profile S; ONVIF Profile G; ONVIF Profile T GB/T 28181
Wejście audio	1
Wyjście audio	1
Obudowa zewnętrzna	IP66, NEMA type 4X
Wandaloodporność	IK10

Temperatura pracy	-40 - +55 C
Zasilanie	Sieciowe lub PoE
Gwarancja	5 lat

Wymagania dla kamery kopułowej

Do dozoru przestrzeni wewnętrznych wymaga się wykorzystania kamer kopułkowych wandaloodpornych, o rozdzielczości 5MP. Dla zapewnienia wysokiej jakości obrazu również w ciemności, kamera musi posiadać wbudowany oświetlacz podczerwieni o zasięgu 30m. Zintegrowany obiektyw z możliwością zdalnej regulacji ogniskowej ma dawać możliwość łatwego dopasowania obserwowanej sceny oraz wyostrzenia obrazu z kamery.
Z racji dużej liczby kamer w systemie security, celem zachowania efektywności systemu bez znaczącego zwiększenia liczby operatorów przyjmuje się aktywne wykorzystanie mechanizmów zaawansowanej analizy obrazów dla kamer CCTV. Tym samym wszystkie kamery w systemie będą fabrycznie wyposażone w funkcje inteligentnej analizy obrazu – nie wymaga to zakupu i uruchamiania dodatkowych licencji. Analiza obrazu ma odbywać się bezpośrednio w kamerze, dzięki czemu zapewniona jest najwyższa skuteczność (praca na nieskompresowanym obrazie) oraz skalowalność. Zakłada się wykorzystanie co najmniej następujących algorytmów analizy:

- Wykrywanie porzucenia przedmiotów
- Wejście w zastrzeżoną strefę
- Zliczanie obiektów
- Nienaturalne szwędanie się osób w wyznaczonych obszarach

W celu znacznie skuteczniejszego wykorzystania funkcji inteligentnej analizy obrazu, kamera ma być w stanie automatycznie sklasyfikować rozpoznany obiekt (jako człowieka, rowerzystę, czy samochód). Rodzaj obiektu będzie wskazany na obrazie poprzez wyświetlanie odpowiedniej ikonki, obok dokładnego obrysu obiektu.

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

Celem zwiększenia efektywności i skrócenia czasu przeszukiwania nagrań przez operatorów, algorytmy inteligentnej analizy obrazów wykorzystywane będą również do analizy wstecznej. Na podstawie metadanych zbieranych w systemie analityki, operator będzie w stanie szybko przeszukać zapisy pod kątem zdarzeń takich jak:

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

Istotną kwestią będzie także cyberbezpieczeństwo całego układu sieciowego i wszystkich systemów security bazujących na nim. Wymaga się szyfrowania komunikacji pomiędzy kamerami, serwerem zarządzającym, stacjami operatorskimi i systemem zapisu, przy wykorzystaniu algorytmów szyfrujących AES z kluczem 256 bit.

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

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

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

Wymagania techniczne:

Parametr	**Wymagania minimalne**
Budowa	Kamera kopułkowa wandaloodporna
Rozdzielczość	3072 x 1728p30
Przetwornik	CMOS 1/2,9"
Czułość	Nie gorsza niż 0,24 lux w trybie dziennym i 0,03 lux w trybie nocnym dla obrazu 30IRE, reflektancji sceny 89%, F1.3 0,0 lux przy włączonym oświetlaczu IR
Zakres dynamiki	120 dB
Kompresja	H.265; H.264; M- JPEG
Obszary ROI	Do 8 obszarów z niezależnymi ustawieniami jakości kodowania
Stosunek sygnał/szum	>55 dB
Migawka	Tryby migawki: automatyczna, wybierana ręcznie.
Oświetlacz IR	Wbudowany, o zasięgu 30 m, z regulacją intensywności
Obiektyw	Zintegrowany 3 - 10 mm ze zdalną regulacją zoom i autofocusem
Obsługiwane protokoły	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/ RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP, FTP, ARP, DHCP, APIPA (Auto-IP, link local address), NTP (SNTP), SNMP (V1, V3, MIB-II), 802.1x, DNS, DNSv6, DDNS, SMTP, iSCSI, UPnP (SSDP), DiffServ (QoS), LLDP, SOAP, Dropbox™, CHAP, digest authentication
Bezpieczeństwo danych	Wsparcie uwierzytelnienia poprzez protokół EAP-TLS 1.0 także z możliwością wgrania certyfikatu w zakresie infrastruktury klucza publicznego do szyfrowania cyfrowego dostarczonego przez producenta kamery, tworzonego przez użytkownika oraz certyfikowane rozwiązania firm 3-ch
	Wsparcie szyfrowania na poziomie sprzętowym tj fabrycznie zabudowany moduł TPM (Trusted Platform Module), który wykorzystuje klucz kryptograficzny do ochrony wszystkich zarejestrowanych danych
Autentykacja wideo	Znak wodny, SHA-1, SHA-256
Łącze sieciowe	RJ-45 100 Base-TX Ethernet
Strumienie wideo	Możliwość generowania 4 strumieni wideo
Inteligentna analiza obrazów	Wbudowana w kamerę z możliwością równoległej analizy do 8 reguł alarmowych
	Analizowane algorytmy: • wykrycie obiektu • przekroczenie linii • kierunkowość ruchu • porzucenie obiektu • zmiana stanu obiektu • zliczanie – przekroczenie linii • zliczanie obiektów w określonych strefach
	Zaawansowane funkcje w zakresie kalibracji i monitorowania obiektu takie jak np. ustalone proporcje

	obiektu, kolor obiektu oraz kierunek i prędkość jego przemieszczania
	Możliwość prezentowania statystyki dla wybranego pola lub obiektu z możliwością odczytu rzeczywistych wartości takich jak prędkości obiektu, jego proporcje i kolor czy kierunek jego poruszania
	Możliwość analizy materiału zarejestrowanego na podstawie metadanych
Zapis lokalny	Wbudowany slot karty SD/microSD (obsługa kart do 2 TB)
Pre-alarm	60s
Zgodność	ONVIF Profile S; ONVIF Profile G
Wejście alarmowe	1
Wyjście przekaźnikowe	1
Wejście audio	1
Wyjście audio	1
Alarm audio	Alarm na podstawie wykrycia dźwięku
Maski prywatności	8
Temperatura pracy	-40 - +50 ºC
Stopień ochrony	IP66
Wandaloodporność	IK10
Zasilanie	Sieciowe lub PoE
Gwarancja	5 lat

Wymagania dla kamery PTZ

Do dozoru terenów zewnętrznych wymaga się wykorzystania, szybkoobrotowych kamer z zoomem 30x, pracujących w rozdzielczości FullHD. Kamery posiadały będą przetworniki o wysokiej czułości gwarantując do 0,004 luxa w trybie nocnym. Kamery wyposażone powinny być we wbudowany i adaptacyjny oświetlacz podczerwieni o zasięgu do 180m.

Z racji dużej liczby kamer w systemie security, celem zachowania efektywności systemu bez znaczącego zwiększenia liczby operatorów wymaga się aktywnego wykorzystania mechanizmów zaawansowanej analizy obrazów dla kamer CCTV, także dla kamer obrotowych. Tym samym wszystkie kamery w systemie będą wyposażone w funkcje inteligentnej analizy obrazu – nie wymaga to zakupu i uruchamiania dodatkowych licencji. Analiza obrazu ma odbywać się bezpośrednio w kamerze, dzięki czemu zapewniona jest najwyższa skuteczność (praca na nieskompresowanym obrazie) oraz skalowalność. Zakłada się wykorzystanie co najmniej następujących algorytmów analizy:

- Wykrywanie porzucenia przedmiotów
- Wejście w zastrzeżoną strefę
- Zliczanie obiektów
- Nienaturalne szwędanie się osób w wyznaczonych obszarach

W celu znacznie skuteczniejszego wykorzystania funkcji inteligentnej analizy obrazu, kamera będzie w stanie automatycznie sklasyfikować rozpoznany obiekt (jako człowieka, rowerzystę, czy samochód). Rodzaj obiektu ma być wskazany na obrazie poprzez wyświetlanie odpowiedniej ikonki, obok dokładnego obrysu obiektu.

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

Kamery obrotowe, odtwarzając sekwencję w prepozycjach, będą aktywnie zbierały informacje o podejrzanych zachowaniach, filtrując tym samym zdarzenia dla operatorów i kierując ich uwagę na

konkretne punkty obserwacji. W przypadku wykrycia niepożądanej aktywności kontrolę nad kamerą będzie mógł przejąć operator.

Celem zwiększenia efektywności i skrócenia czasu przeszukiwania nagrań przez operatorów, algorytmy inteligentnej analizy obrazów wykorzystywane będą również do analizy wstecznej. Na podstawie metadanych zbieranych w systemie analityki, operator będzie w stanie szybko przeszukać zapisy pod kątem zdarzeń takich jak:

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

Istotną kwestią będzie także cyberbezpieczeństwo całego układu sieciowego i wszystkich systemów security bazujących na nim. Wymaga się szyfrowania komunikacji pomiędzy kamerami, serwerem zarządzającym, stacjami operatorskimi i systemem zapisu, przy wykorzystaniu algorytmów szyfrujących AES z kluczem 256 bit.

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

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

Kamera ma dawać możliwość skonfigurowania do 32 masek prywatności. Aby zapewnić odpowiednią czytelność obrazu mają być dostępne do wyboru 3 kolory masek, w tym maska zlewająca się z kolorem tła.

Wymagania techniczne:

Parametr	**Wymagania minimalne**
Budowa	Kamera szybkoobrotowa z oświetlaczem
Rozdzielczość	1920 x 1080p60
Przetwornik	CMOS 1/ 2,8"
Zoom optyczny	30x (4,5 - 135mm)
Zoom cyfrowy	16x
Czułość	Nie gorsza niż 0,019 lux w trybie dziennym i 0,004 lux w trybie nocnym dla obrazu 30IRE, przy migawce 1/30 s, reflektancji sceny 89%
Oświetlacz IR	Wbudowany 850 nm o zasięgu do 180 m
Stosunek sygnał/szum	>55 dB
Zakres dynamiki	120 dB
Kompresja	H.265, H.264, M-JPEG
Obrót	360°, ciągły
Prędkość obrotu	Zmienna 0,1°/s – 240 °/s (obrót)
Obsługiwane protokoły	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP,FTP, ARP, DHCP, APIPA, NTP (SNTP), SNMP (V1, V3, MIB-II),802.1x, DNS, DNSv6, DDNS, SMTP, iSCSI,UPnP (SSDP), DiffServ (QoS), LLDP, SOAP,Dropbox™, CHAP, digest authentication
Bezpieczeństwo danych	Wsparcie uwierzytelnienia poprzez protokół EAP-TLS 1.0 także z możliwością wgrania certyfikatu w zakresie infrastruktury klucza publicznego do szyfrowania cyfrowego dostarczonego przez producenta kamery, tworzonego przez użytkownika oraz certyfikowane rozwiązania firm 3-ch

	Wsparcie szyfrowania na poziomie sprzętowym tj fabrycznie zabudowany moduł TPM (Trusted Platform Module), który wykorzystuje klucz kryptograficzny do ochrony wszystkich zarejestrowanych danych
Autentykacja wideo	Znak wodny, SHA-1, SHA-256
Łącze sieciowe	RJ-45 100 Base-TX Ethernet
Strumienie wideo	Możliwość generowania 4 strumieni wideo
Inteligentna analiza obrazów	Wbudowana w kamerę z możliwością równoległej analizy do 16 reguł alarmowych
	Programowana niezależnie dla co najmniej 8 prepozycji kamery
	Analizowane algorytmy: • wykrycie obiektu • przekroczenie linii • kierunkowość ruchu • porzucenie obiektu • zmiana stanu obiektu • zliczanie – przekroczenie linii • zliczanie obiektów w określonych strefach
	Zaawansowane funkcje w zakresie kalibracji i monitorowania obiektu takie jak np. ustalone proporcje obiektu, kolor obiektu oraz kierunek i prędkość jego przemieszczania
	Możliwość prezentowania statystyki dla wybranego pola lub obiektu z możliwością odczytu rzeczywistych wartości takich jak prędkości obiektu, jego proporcje i kolor czy kierunek jego poruszania
	Możliwość analizy materiału zarejestrowanego na podstawie metadanych
Zapis lokalny	Wbudowany slot karty SD/microSD (obsługa kart do 2 TB)
Zgodność	ONVIF Profile S, ONVIF Profile G, ONVIF Profile T
Wejście alarmowe	2
Wyjście przekaźnikowe	1
Wejście audio	1
Programowalne prepozycje	256
Trasy dozorowe	2
Maski prywatności	32
Obudowa zewnętrzna	IP66
Temperatura pracy	-40 - +60 st. C
Zasilanie	Sieciowe lub PoE
Gwarancja	3 lata

Minimalne wymagania dla stacji roboczej.

- Do obsługi systemu monitoringu wizyjnego wymaga się dedykowanych stacji roboczych wysokiej wydajności, umożliwiających jednoczesne wyświetlanie kilkudziesięciu obrazów z kamer wysokiej rozdzielczości.
- Stacja robocza umożliwi jednoczesne podłączenie do 4 monitorów wysokiej rozdzielczości.
- Stacja ma być wyposażona w wydajną kartę graficzną NVIDIA Quadro RTX 4000 z wbudowaną pamięcią 8GB, wspierającą dekodowanie sprzętowe (GPU) obrazu z kamer wyświetlanych w oprogramowaniu klienckim systemu monitoringu wizyjnego.

- Stacja ma być wyposażona w fabrycznie instalowany system operacyjny Windows 10 Professional 64-bit
- Stacja robocza ma być wyposażona w wydajny zasilacz o skuteczności co najmniej 90% i o mocy co najmniej 750 W.
- Stacja robocza ma być objęta co najmniej 3-letnią gwarancją Next Business Day.
- Podstawowe wymagane parametry techniczne stacji roboczej zestawiono w poniższej tabeli:

Parametr	**Wymagania minimalne**
Funkcja	Stacja robocza aplikacji klienckiej systemu monitoringu wizyjnego
Oprogramowanie	Oprogramowanie klienckie systemu zarządzania wideo, zgodne z wymaganiami dla VMS
Procesor	Intel Xeon W-2123 (3,6 GHz, 8,25 MB cache, pamięć 2666 MHz, 4-rdzeniowy)
Karta graficzna	NVIDIA Quadro RTX 4000, 8GB
Pamięć	8 GB (1 x 8 GB) DDR4 2666 DIMM ECC RAM
Dysk twardy	500 GB, 7200 RPM SATA 3,5”
Zasilacz	750W, wydajność 90%
Obudowa	Minitower
System operacyjny	Windows 10 Professional 64-bit

2. Minimalne wymagania dla Systemu SKD i SSWiN (Grade 3)

- Dostarczony system ma cechować się bardzo dużym stopniem stabilności i redundancji, ma być zgodny, tożsamy i kompatybilny z systemem już wdrożonym na innych obiektach należących do ENEA Nowa Energia Sp. z o.o. Warunkiem koniecznym jest zapewnienie w systemie autonomicznego działania kontrolerów. Oznacza to, że:
  - Kontrolery muszą być standardowymi urządzeniami sieciowymi (posiadającymi możliwość komunikacji z innymi urządzeniami w sieci TCP/IP, bez konieczności stosowania jakiejkolwiek formy konwersji sygnału.
  - Kontrolery będą komunikować się z innymi kontrolerami na zasadzie „peer to peer” (bez pośrednictwa serwera)
  - Kontrolery muszą posiadać dużą moc obliczeniową (CPU minimum 800MHz) i duże zasoby pamięci (min. 256 MB SDRAM, 2 GB pamięci typu Flash).
  - Komunikacja w systemie musi odbywać się z wykorzystaniem protokołu TCP/IP w sposób szyfrowany i zabezpieczony protokołem SSL/TLS i szyfrem co najmniej 128 bitowym.
  - Wszystkie kontrolery sieciowe muszą wspierać model uwierzytelniania 802.1x, celem wyeliminowania niebezpieczeństwa polegającego na nieautoryzowanym dostępie do sieci już na poziomie warstwy dostępu do sieci.
- Monitorowanie urządzeń powinno zostać zrealizowane poprzez protokół SNMP lub równoważny.
- Logowanie do systemu musi być zabezpieczone indywidualnym loginem i hasłem, przy czym system musi pozwalać na wymuszenie przez administratora stosowania haseł o określonej sile oraz ich zmianę po określonym interwale czasowym.

- Logowanie do aplikacji systemu kontroli dostępu musi wspierać mechanizm podwójnej autentykacji tzw. Two-factor authentication (2FA).
- System musi zapewniać swobodne programowanie funkcjonalności (na poziomie kontrolera)z poziomu prostej aplikacji graficznej za pomocą metod „drag and drop".
- Wymagamy Karty Mifare Plus X (Chip w kartach PKI), których z automatu wgrany jest klucz szyfrujący i w naszej instancji KD AEOS dostęp jest możliwy jedynie poprzez te klucze. Kluczem tym zarządza IT Enea Centrum , co jest jednym z elementów spełnienia wymogów dyrektywy NIS2 dla firm energetycznych.

Minimalne wymagania dla projektowanego środowiska serwerowego:

- Serwer produkcyjny ma działać w klastrze HA (w razie uszkodzenia 1 węzła zostaje uruchomiony drugi).
- Środowisko serwerowe musi składać się z:
    - Serwera aplikacji umożliwiającego pracę w dowolnym systemie wspomaganym przez Java.
    - Relacyjnej bazy danych (serwera bazodanowego) wykorzystującego język zapytań SQL.
- Wdrażane środowisko serwerowe powinno spełniać następujące minimalne wymagania sprzętowe:
    - Nowoczesna 64 bitowa maszyna serwerowa (zastosowane serwery będą serwerami wirtualnymi w środowisku VMWare.).
    - Jeden z poniższych systemów operacyjnych:
      - Microsoft Windows Server 2016R2 lub 2019.c) Jedna z poniższych baz danych:
      - Oracle® 18c Enterprise edition lub wyższa.
      - MS SQL Server 2014[1]/2016/2017/2019[3], wersja Standard lub Enterprise (nie akceptowalna wersja Express)
      - MySQL Enterprise Edition 5.5/5.6/5.7
      - PostgreSQL wersja 9.x/10.x
- Aplikacja Kliencka/Operatorska musi: Umożliwiać dostęp do systemu dla Użytkownika (role typu: Administrator, Operator, Recepcja) z poziomu przeglądarki internetowej – brak konieczności instalowania dodatkowego, dedykowanego oprogramowania na stacjach roboczych.
    - Wspierać minimum poniżej wskazane przeglądarki:
    - Microsoft Internet Explorer.
    - Firefox.
    - Chrome.

Wymagania dotyczące kontrolerów:

- Kontrolery muszą zapewniać możliwość autonomicznego podejmowania decyzji o autoryzacji bez udziału serwera (informacje niezbędne do autoryzacji opcjonalnie mogą być przechowywane również w pamięci kontrolerów, a nie tylko na serwerze).
- Kontrolery muszą buforować co najmniej 1 000 000 zdarzeń pracując w trybie autonomicznym.
- Buforowane zdarzenia muszą być automatycznie przesyłane, po odzyskaniu łączności z serwerem.

- Kontrolery muszą mieć możliwość bieżącego przekazywania informacji o stanach czujników (np. kontaktronów drzwiowych) również podczas braku dostępu do serwera.
- Kontrolery systemu muszą posiadać możliwość pracy w trybie autonomicznym. Oznacza to, że w sytuacji braku dostępu do serwera z jednej strony będą one w stanie przejąć na siebie rolę bezpośredniej komunikacji między sobą i będą przesyłać na bieżąco informacje o stanach przejść (drzwi otwarte/drzwi zamknięte, drzwi otwarte zbyt długo, drzwi sforsowane itp.) do własnego systemu monitorującego lub do zewnętrznych zintegrowanych systemów monitorujących.
- Jeden kontroler musi umożliwiać podłączenie minimum 31 modułów kontroli dostępu co pozwala na obsłużenie 32 przejść pojedynczych lub podwójnych.
- Jeden kontroler wraz z modułami dostępu umożliwi obsłużenie minimum 64 czytników kart.
- Zmiana oprogramowania czy konfiguracji systemu musi być możliwa dla całego systemu z jednego centralnego punktu lub dla wybranych elementów/modułów lokalnie lub centralnie. Możliwe musi być zdalne sprawdzenie pełnej konfiguracji zapisanej w pamięci wybranego kontrolera (poprzez graficzne narzędzie pozwalające na monitorowanie działania systemu w trybie na żywo – np. przyłożenie identyfikatora do czytnika spowoduje zaznaczenie całej ścieżki sygnału w systemie od czytnika, poprzez moduł czytnika aż do kontrolera).
- System musi być wykonany w oparciu o architekturę gwiazdy przy użyciu tylko kontrolerów, połączonych bezpośrednio do przełączników sieciowych. W architekturze systemu mogą być użyte tylko kontrolery, bez modułów rozszerzeń.
- Dostarczony system musi posiadać integracje z systemem wdrożonym w GK ENEA platformy integrującej potwierdzoną przez producenta tego systemu w zakresie:
    - Wizualizacji stanów pracy: otwarcie przejścia za pomocą karty, udzielenia dostępu do KD przez administratora, zakluczenia drzwi których zamki wysyłają takie stany oraz stan awarii.
    - Sterowania przejściami: otwarcie, zamknięcia drzwi,
- Kontrolery muszą posiadać obok standardowego wejścia zasilającego 12-24 VDC, możliwość zasilania za pomocą standardu PoE+ (Power over Ethernet IEEE 802.3at).

Wymagania dotyczące oprogramowania aplikacyjnego:

- System musi posiadać, co najmniej trzy rodzaje oprogramowania aplikacyjnego lub zapewniać, w zależności od uprawnień osoby zalogowanej do aplikacji uzyskanie co najmniej trzech poziomów zarządzania systemem:
    - Poziom administratora.
    - Poziom rozszerzony użytkownika (możliwość zarządzania alarmami, drzwiami, możliwość dodania komentarza dla poszczególnych alarmów).
    - Poziom ograniczony użytkownika (informacja o stanie autoryzacji wraz z prezentacją miejsc w których autoryzacja bądź jej brak miała miejsce).
- Oprogramowanie najwyższego poziomu musi zawierać wbudowany moduł obsługi i monitorowania alarmów i stanów czujników Systemu Kontroli Dostępu. W module tym musi być możliwość przypisywania do konkretnych alarmów/zdarzeń określonych procedur. W ramach procedur alarmowych wyświetlane muszą być przygotowane wcześniej instrukcje alarmowe, a w określonych przypadkach, system musi wymuszać opatrzenie alarmu komentarzem i zestawem komentarzy pracownika ochrony pełniącego służbę na stanowisku monitoringu obiektowego. System musi umożliwiać również

automatyczne pokazanie podglądu z kamery wideo, która jest skojarzana z punktem alarmowym np. główne wejście do budynku.

- Oprogramowanie niższego poziomu musi wykorzystywać do komunikacji pomiędzy systemem a użytkownikiem przede wszystkim elementy graficzne takie jak ikony, okna i przyciski. System musi pozwalać na podłączanie skanerów dokumentów co najmniej kilku różnych producentów, dzięki którym możliwe będzie wprowadzanie danych osobowych poprzez skanowanie dokumentów potwierdzających tożsamość. Oprogramowanie musi posiadać możliwość obsługi czytników kart dla biur przepustek. Oprogramowanie musi zapewniać możliwość wprowadzania tzw. pól dowolnych (np. PESEL itp.) Oprogramowanie musi pozwalać na ograniczanie dostępnych funkcjonalności w zależności od uprawnień i obowiązków użytkownika logującego się do systemu.
- Wszelkie informacje wyświetlane w oprogramowaniu muszą być dostępne w języku polskim i zawierać polskie znaki diakrytyczne.
- Poza standardowymi funkcjami oprogramowania systemu KD dotyczącymi nadawania posiadaczom identyfikatorów i uprawnień dla poszczególnych przejść zgodnie z określonymi harmonogramami czasowymi, system musi pozwalać na realizację poniższych funkcjonalności:
    - Kontrola obchodu strażników (z możliwością swobodnego kształtowania tras obchodu i okien czasowych dla poszczególnych punktów kontrolnych – czytników).
    - Automatyczne blokowanie identyfikatorów po określonym czasie nieużywania.
    - Tworzenie profili tymczasowych tzn. zmiana profilu na określony czas, po którym automatycznie zostanie przywrócony poprzedni profil.
    - Blokowanie identyfikatorów w wyniku określonych naruszeń instrukcji ruchu osobowego np. złamanie zasady antypassback.
    - System musi pozwalać na automatyczne usuwanie danych odwiedzających po definiowalnym okresie czasu.
    - Tekstowy monitor zdarzeń – bieżące wyświetlanie wszystkich zdarzeń w systemie w formie tekstowej.
    - Rozbudowany monitor zdarzeń – bieżące wyświetlanie zdarzeń w systemie z towarzyszącymi im zdjęciami (zdjęcia osób wyświetlane w tym samym momencie co zbliżenie identyfikatora do czytnika).
    - Tworzenie tzw. czarnych list.
    - Awizowanie wizyt gości/firm zewnętrznych przez pracowników posiadających dostęp do systemu.
    - Zliczanie osób w określonej strefie i wprowadzanie ograniczeń liczby osób uprawnionych do przebywania w strefie.
    - Tworzenie wydzielonych wirtualnie części systemu dla poszczególnych oddziałów, dzięki czemu użytkownicy w poszczególnych oddziałach będą mieli możliwość nadawania uprawnień jedynie osobom przypisanym do swojego oddziału. Wybrani użytkownicy systemu będą mogli kształtować uprawnienia wszystkich osób.
    - Stosowanie filtrów przejść, dzięki czemu użytkownicy systemu w poszczególnych oddziałach będą mieli dostęp do przejść przypisanych jedynie do ich oddziału.
    - Ograniczenie liczby zbliżeń identyfikatora do czytników, dzięki czemu możliwe musi być wymuszenie właściwej ścieżki poruszania się po obiekcie – jeżeli na drodze od wejścia głównego do pomieszczenia, które jest celem wizyty znajdują się 4 czytniki możliwe musi być ograniczenie tej liczby do 4, co wyeliminuje ryzyko nieuprawnionego poruszania się osoby po obiekcie.

- System KD musi mieć możliwość łączenia zdarzeń tekstowych (np. autoryzacja, otwarcie drzwi itp.) wraz ze zdjęciami poszczególnych użytkowników oraz ujęciem na żywo z kamery, aby móc w trybie rzeczywistym porównać prezentowane dane.
- Możliwość importu danych osobowych z innego zewnętrznego źródła (np. baza danych działu personalnego) w minimum standardzie pliku xlsx.
- System musi umożliwiać integracje z LDAP.
- System KD musi umożliwiać zastosowanie funkcjonalności ANTYPASSBACK - uniemożliwia dwukrotne wejście posiadacza do danej strefy bez jej opuszczenia albo użycia niedozwolonego przejścia. APB zapobiega autoryzowanemu wejściu do budynku, strefy lub obszaru przez osobę korzystającą z identyfikatora należącego do osoby już będącej w środku.
- System CSKD musi umożliwiać zastosowanie następujących trybów antypassback: - Miękki APB (ANTYPASSBACK)– generuje zdarzenie alarmowe po naruszeniu zasady.
  - Twardy APB (ANTYPASSBACK– nie wpuszcza karty z wewnątrz strefy do tej samej strefy - Czasowy APB (ANTYPASSBACK) – możliwy reset osoby po określonym czasie od wejścia
- Infrastruktura IT GK ENEA oparta jest o platformę wirtualizacją VMware vSphere.
- Serwery systemu KD będą również zwirtualizowane na tej platformie, zarówno środowisko testowe i produkcyjne.
- System ma być zbudowany o klastry HA tak aby wyeliminować pojedyncze punkty awarii.
- System musi posiadać architekturę rozproszoną między CPD w GK ENEA (Poznań – Koronowo - Pieczyska – Tryszczyn – Smukała - Radom).
- Pod instalację systemu KD zostanie udostępniona licencja Windows Server 2016 lub 2019.
- System musi być oparty o czytniki obsługujące karty w standardzi Desfire EV1.
- Systemu musi umożliwiać podłączenie dowolnych czytników kart obsługujące inne standardy ale za pomocą bezpiecznego interfejsu (szyfrowanego) np.: OSPD w wersji 2.
- W ramach dostawy zostaną dostarczona drukarka do wydawania przepustek na kartach stałych.
- Systemy musi obsługiwać :
  - <20 tysięcy użytkowników.
  - nadzorować < 1500 przejść.
  - umożliwiać praca kontrolerów on line lub autonomiczną.
  - pojemność zapisu zdarzeń w trybie ON-LINE min. Na okres 12 miesięcy.
  - możliwość określenia 120 dni wolnych.
  - funkcja Anti-pass-back.
  - zakres temperatur pracy czytników – do -20 oC +50 oC.
  - monitorowane wejścia czujników drzwi, przycisków wyjścia, itd.
  - współpraca z czytnikami biometrycznymi firm: Suprema, Touchless Biometric System.
  - Współpraca z rozwiązaniami biometrycznymi umożliwiającymi rozpoznawanie twarzy firm: Thales, OOSTO, Suprema.
  - możliwość kontroli wind.
- Czas na czytnikach ma być uregulowany i zsynchronizowany z wewnętrznym serwerem NTP GK ENEA.

  - System musi posiadać przejrzysty interfejs nadawania uprawnień do stref z poziomu widoku użytkownika.
- System ma mieć możliwość blokowania wejścia dla wybranych osób zgodnie z harmonogramem lub całkowitego zablokowania możliwość wejścia na obiekt.
- System SKD musi zapewniać dedykowane zabezpieczenia chroniące przed atakami sieciowymi, polegające na wyposażeniu kontrolera drzwiowego w moduł, który umożliwia przechowywanie certyfikatów uwierzytelniających komunikację między serwerem zarządzającym Systemem Kontroli Dostępu a kontrolerami drzwiowymi. Takie rozwiązanie wymusza autentykacje nowych kontrolerów przez administratora zanim zostaną dodane do Systemu Kontroli Dostępu, a tym samym zabezpiecza przed nieautoryzowanym zmodyfikowaniem oprogramowania zarządzającego kontrolerem.
  - Klucze szyfrujące Mifare DESSFire odpowiadające za odczyt danych autoryzacyjnych z karty RFID, mają posiadać opcję przechowywania w tym samym dedykowanym module kontrolera drzwiowego co certyfikaty autentykacyjne. W takim scenariuszu czytnik staje się dla karty transparentny i deszyfracja następuje po stronie kontrolera.
  - Zarządzanie certyfikatami autentykacyjnymi jak i kluczami DESFire ma być możliwe z centralnego poziomu, jednej stacji roboczej. Certyfikaty i klucze mają posiadać możliwość automatycznego dystrybuowanania do kontrolerów drzwiowych z jednego punktu zarządzania do wszystkich elementów systemu KD.
  - Zamawiający ma mieć możliwość zarządzania i wymiany certyfikatów autentykacyjnych w każdym momencie bez ingerencji dostawcy systemów.
- Wspólna baza użytkowników dla systemu SSWiN i SKD.
- Wspólna baza zdarzeń.
- Współgranie zdarzeń pomiędzy systemami SKD<->SSWIN – możliwość tworzenia nieograniczonych wzajemnych relacji – w sposób cyfrowy np.:
  - Automatyczne zazbrojenie gdy ostatnia osoba wyszła a czujniki PCP nie wykazują ruchu przez określony czas.
  - Automatyczne rozbrojenie, gdy osoba upoważniona posiada autoryzację do danej strefy.
- Jeden interfejs komunikacyjny (API) dla integracji z systemami zewnętrznymi.
- Korzystanie z tych samych czytników w zakresie SSWiN i SKD
- Jedno miejsce zarządzania uprawnieniami.
- Tworzenie wspólnych raportów.
- Wymaga się szyfrowanej komunikacji na każdym etapie: Aplikacje klienckie <-> Server <-> Kontroler drzwiowy <-> czytnik <-> karta.
- Wymaga się wykonania Systemu Kontroli Dostępu w trybie transparentnym: czyli przeniesienie kluczy szyfrujących z czytnika, na kontroler drzwiowy (który jest instalowany po bezpiecznej stronie: wewnętrzna strona drzwi, serwerownia czy szacht teletechniczny). W takim rozwiązaniu nie ma informacji wrażliwych (klucze DESFire) na zewnątrz obiektu co podnosi znacząco poziom bezpieczeństwa.

- Wymaga się przez system KD dwuetapowego uwierzytelniania: dwustopniowy poziom logowania do aplikacji zarządzających. Podajemy nazwę użytkownika, hasło + hasło generowane jednorazowo przez aplikacje typu OKTA czy Microsoft Authenticator

- Wymaga się w Systemie Kontroli Dostępu stosowania protokołu 802.1X dla kontrolerów. Co umożliwi uwierzytelnianie kontrolerów na poziomie warstwy sieciowej. W praktyce oznacza to, iż nie wepniemy kontrolera do sieci, jeśli nie otrzyma on odpowiednich certyfikatów uwierzytelniających.

Czytniki

Należy stosować czytniki kompatybilne z zastosowanym systemem. Wykorzystywane czytniki muszą posiadać możliwość odczytu karty wyspecyfikowanej w punkcie poniżej. Komunikacja pomiędzy kontrolerem a czytnikiem musi odbywać się kanałem szyfrowanym – co najmniej za pomocą szyfrowanego standardu OSDP lub w przypadku wykonania systemu w standardzie end-to-end security w kodowanym protokole własnym producenta systemu.

- Kompatybilność z EN50131 Grade 3
- Interfejs RS485
- Wyświetlacz graficzny
- Podświetlana klawiatura dotykowa

Kontrolery

- Ethernet 10/100Mbit. Komunikacja z AEOS, AEpu,
- PoE+
- Magistrala RS485 komunikacyjna
- 2x RS485, lub 2 x Wiegand (128Bit) – interfejsy czytników
- 6 nadzorowanych wejść
- 2 dodatkowe wejścia AC OK., BAT OK
- 6 wyjść OK.
- 2 wyjścia RELAY
- Monitorowane wyjścia zasilające
- Procesor 800MHz, 256MB RAM, 2GB Flash
- Zasilanie 12-24V DC
- Zegar czasu rzeczywistego
- Max 31 rozszerzeń

Centrala alarmowa

- Kompatybilność z EN50131 Grade 3
- Izolowana magistrala AEbus (CAN)
- 16 nadzorowanych wejść 3EOL, 2EOL, EOL, NO, NC (konfigurowalna wartość rezystancji)
- 2 wyjścia przekaźnikowe i 8 wyjść OC
- Interfejs klawiatur RS485
- Zasilanie 230VAC, 24VDC 17Ah
- Izolator magistrali CAN

- Integracja z SKD i CCTV, np. zazbrojenie strefy powoduje wyłączenie czytnika na wejściu
- Czujka może należeć do wielu stref
- Korzystanie z tej samej platformy sprzętowej i licencyjnej SKD/SSWiN
- Korzystanie z tej samej bazy danych SKD/SSWiN

3. Minimalne wymagania dla systemu integrującego systemy ZSB

System zarządzania bezpieczeństwem ma być systemem otwartym, zgodnym z obecnie funkcjonującym i wdrażanym systemem zarządzania bezpieczeństwem na obiektach Enei Nowej Energii tzn. umożliwić rozbudowę o nowe elementy systemów bezpieczeństwa i technicznych obiektu. System zagwarantuje możliwość pracy jednostanowiskowej i sieciowej, z możliwością podziału zadań pomiędzy poszczególne stacje robocze – inne uprawnienia, wizualizacje i komunikaty dla służb ratowniczych, technicznych, ochrony, itp.
Oferowany system integrujący powinien posiadać ważną Krajową Ocenę Techniczną, Certyfikat Stałości Właściwości Użytkowych, Świadectwo Dopuszczenia do stosowania w ochronie przeciwpożarowej wydane przez jednostkę certyfikującą CNBOP, umożliwiającą współdziałanie (wizualizację i sterowanie) wszystkich systemów, których działanie lub dezaktywacja dla Systemów Wykrywania i Sygnalizacji Pożaru.
Należy zastosować dedykowaną aplikację mobilną instalowaną na urządzeniach przenośnych (np. smartfon).
System nadrzędny ma umożliwiać przekazywanie zdarzeń w celu obsługi operatorom mobilnym wyposażonym w PDA (Personal Digital Assistant).

- System zarządzania musi być neutralny wobec producentów integrowanych systemów i urządzeń.
- System zarządzania musi być wyposażony w dedykowany moduł raportujący.
- System zarządzania musi być wyposażony w moduł powiadamiania SMS.
- Wymagane jest aby system PSIM **(Physical Security Information Management)** zapewnił dwukierunkową kontrolę zarządzanych systemów i informacji zarządczej. Rozumie się przez to możliwość sterowania zintegrowanymi systemami np. nadawanie uprawnień w systemie kontroli dostępu, blokowanie czujek systemu ppoż., sterowanie kamerami.
- Wymagane jest aby system PSIM wspierał wymianę informacji z użytkownikami mobilnymi opartymi o Android.
- Oprogramowanie musi mieć budowę modułową. Wymiana dowolnego modułu programowego nie może wstrzymywać pracy pozostałych modułów i funkcji systemu.
- 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 musi pracować w sieci komputerowej oraz zapewniać pełną obsługę za pomocą przeglądarki internetowej z dowolnego miejsca w sieci, w tym administrowanie systemem.
- System integracyjny PSIM ma być tożsamy z już wdrożonym systemem na obiektach należących do Enea Nowa Energia.
- Wymagane jest aby każda czynność wykonywana przez użytkownika w systemie PSIM była rejestrowana w bazie danych.
- Wymagana jest możliwość skonfigurowania systemu z wieloma stanowiskami roboczymi.
- Oprogramowanie musi mieć możliwość pracy w środowiskach wirtualnych, pozwalając tym samym na wizualizację i integrację z platformą zarządczą środowiska wirtualnego.
- Niedopuszczalnym jest aby aktualizacja systemu PSIM powodowała wyłączenie serwera aplikacji na czas aktualizacji lub modernizacji oprogramowania.
- Wymaga się aby system PSIM wspierał pracę w środowiskach jedno i wieloprocesorowych - optymalnie wykorzystując konfigurację sprzętową.
- Wymagane jest zapewnienie mechanizmów automatycznego i ręcznego kopiowania dowolnych danych lokalnie lub na zdalny serwer.
- System PSIM musi zapewnić rozszerzenie o obsługę nowych urządzeń poprzez dodanie sterownika programowego do serwera aplikacji.
- Wymagane jest aby zdarzenia i reakcje na zdarzenia były zapamiętywane w logu działań, wraz z możliwością ich raportowania.
- Wymaga się aby PSIM był rozwiązaniem skalowanym i elastycznym, umożliwiającym rozbudowę funkcjonalności i pojemności stopniowo - rozszerzając zakres licencjonowania oprogramowania na żywo bez konieczności przerywania pracy systemu.
- Wymagane jest, aby system PSIM posiadał rozbudowany system poziomów dostępu dla poszczególnych grup użytkowników z możliwością zróżnicowania uprawnień dostępu do,

nie mniej niż 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 w zakresie: brak dostępu, tylko odczyt, edycję, wprowadzanie nowych, kasowanie

- Wymagana jest możliwość nadawania uprawnień indywidualnie dla każdego elementu w systemie PSIM.
- Wymagane jest, aby system posiadał możliwość przypisywania uprawnień dla operatorów z możliwością tworzenia indywidualnych stanowisk obsługi przypisanych do operatora bądź grupy.
- Wymagana jest 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 połączone z możliwością kierowania zdarzeń na stanowiska robocze. Wymagane jest zróżnicowanie kolorów zdarzeń poszczególnych kategorii.
- Zdarzenia muszą być prezentowane na liście 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 PSIM musi powracać automatycznie do widoku zdarzeń wszystkich

kategorii (widok nie filtrowany) po upływie zadanego czasu.

- Wymagana jest możliwość korelacji zdarzeń i generowania zdarzenia dodatkowego.
- Wymagane jest aby system PSIM umożliwiał filtrowanie aktywnych alarmów dla dowolnego zdarzenia.
- Wymagana jest sygnalizacja przerwy komunikacji z każdym integrowanym systemem poprzez wyświetlenie odpowiedniego komunikatu alarmowego.
- Wymagane jest aby system PSIM automatycznie powracał do stanu pracy. Niezbędne składniki oprogramowania (moduły) muszą być uruchamiane automatycznie (np. usługi systemu operacyjnego).
- Wymagane jest aby system PSIM posiadał plany w formacie wektorowym z możliwością skalowania obrazu dla całego obszaru jak i poszczególnych budynków, stref.
- Wymagane jest, aby czujniki na planie wyświetlane były warstwowo dla poszczególnych systemów, z możliwością wygaszania warstw i zdefiniowanych widoków (wycinków) na wypadek zdarzenia z danego systemu.
- Edycja pliku podkładowego nie może wpływać na zawartość naniesionych warstw graficznych.
- PSIM musi zapewnić mechanizm ukrywania zbędnych w danym momencie okien aplikacji. W przypadku wystąpienia alarmu okna odpowiedzialne za dane podsystemy muszą być przywrócone do głównego widoku.
- Wymaga się aby wszystkie alarmy były wyświetlane w dedykowanych kategoriach z podziałem na lokalizacje. Na wszystkich stacjach roboczych system musi zgłaszać zdarzenia wizualnie i dźwiękowo.
- Wymagane jest, aby system PSIM posiadał możliwość tworzenia raportów dziennych, miesięcznych, kwartalnych ze sprawności integrowanych systemów.
- Wymagane jest, aby PSIM posiadał wbudowane narzędzie do tworzenia planów sytuacyjnych, które musi umożliwić tworzenie przycisków sterujących i elementów funkcyjnych z wykorzystaniem dowolnych czcionek, kolorów, wypełnień, obrazków i animacji.
- Wymagane jest aby system PSIM posiadał możliwość tworzenia indywidualnych procedur działania na wypadek zdarzenia w budynkach objętych nadzorem z możliwością rozgałęzienia procedur na kolejne etapy w zależność od działań podjętych przez operatora.
- Wymagane jest aby system PSIM posiadał możliwość załączania dowolnych dokumentów takich, jak karty katalogowe, instrukcje, przypisanych do konkretnych procedur działania, czujników lub urządzeń.

- PSIM musi zapewnić mechanizm swobodnego kształtowania układu ramek aplikacji tak, aby dowolna zawartość mogła być zagnieżdżana np. w układzie siatki.
- Wymagane jest, aby system PSIM posiadał moduł wprowadzania adresów i kontaktów - baza serwisantów, pojazdów itp.
- Wymagane jest aby system posiadał możliwość podłączenia dowolnego urządzenia lub systemu za pomocą protokołu komunikacyjnego.
- Wymagane jest aby system PSIM posiadał możliwość tworzenia indywidualnych stanowisk obsługi dla poszczególnych budynków jak i możliwość nadzorowania wszystkich budynków z jednej stacji operatorskiej.
- Wymagane jest, aby system PSIM umożliwiał podłączanie dowolnych urządzeń komunikujących się za pomocą styku (sterowanie i nadzorowanie – w tym urządzenia ochrony przeciwpożarowej).
- Wymagane jest, aby instalacja PSIM była zabezpieczona bezpiecznym połączeniem z serwerem za pomocą SSL.
- Wymagane jest, aby system PSIM był utworzony w architekturze klient-serwer w oparciu o technologię Microsoft.NET.
- Wymagane jest zapewnienie możliwości tworzenia makr i formularzy.
- Wymagane jest zapewnienie obsługi PHP, Javascript i Shockwave Flash.
- Wymagane jest aby PSIM stosował zmianę ustawień stylów z formularza CSS.
- Wymagane jest, aby PSIM posiadał wbudowany 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 elementy.
- Wymagana jest możliwość wykonywania backupu online oraz backupu przyrostowego.
- Wymagana jest możliwość backupu bazy danych. Możliwość odtworzenia systemu z backupu.

4. Minimalne wymagania dla systemu aktywnego LAN.

Switch 16-port 10G SFP

Przełącznik typu standalone musi być wyposażony w 16 portów 1/10 Gigabit Ethernet SFP/SFP+

- Przełącznik musi posiadać jeden dodatkowy slot na moduł rozszerzeń. Z dostępnością następujących modułów:
  - Minimum 8-portowy moduł 10Gigabit Ethernet SFP+

- Minimum 2- portowy moduł 40Gigabit Ethernet QSFP

Porty SFP/SFP+ umożliwiają zastosowanie następujących wkładek interfejsowych:

- Gigabit Ethernet 1000Base-T,
- Gigabit Ethernet 1000Base-SX,
- Gigabit Ethernet 1000Base-LX/LH,
- Gigabit Ethernet 1000Base-EX,
- Gigabit Ethernet 1000Base-ZX,
- Gigabit Ethernet 1000Base-BX-D/U,
- 10Gigabit Ethernet 10GBase-SR,
- 10Gigabit Ethernet 10GBase-LR,
- 10Gigabit Ethernet 10GBase-LRM,
- 10Gigabit Ethernet 10GBase-ER,
- 10Gigabit Ethernet 10GBase-ZR,
- 10Gigabit Ethernet 10GBase-BX-D/U,
- 10Gigabit Ethernet typu twinax (SFP+ - SFP+),

Porty QSFP mają umożliwiać zastosowanie następujących modułów interfejsowych:

Dla transmisji 40Gb/s:

- 40G-SR4,
- 40G-LR4,
- 40G-ER4,
- 40G-SR-BD,
- 40G-CSR,
- 40G-CSR4,
- 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652),
- adapter 40G QSFP->10G SFP+,
- 40Gigabit Ethernet typu twinax (QSFP - QSFP);

Urządzenie ma być wyposażone w wymienne moduły wentylatorów,

Urządzenie może zostać wyposażone w zasilacz redundantny do pracy w trybie 1:1;

Urządzenie ma posiadanać 32MB bufor pamięci,

16GB pamięci DRAM i 16GB pamięci flash,

Przepustowość przełącznika (switching capacity) ma wynosić 480 Gbps,

Prędkość przesyłania (forwarding rate) ma wynosić 360 Mpps,

Obsługa:

- 1000 aktywnych sieci VLAN,
- 64 000 adresów MAC,
- 64 000 tras IPv4,
- 32 000 tras IPv6,
- Ilość wpisów w listach kontroli dostępu Security ACL – 18 000,
- ilość wpisów w listach kontroli dostępu QoS ACL – 18 000,
- 1000 interfejsów SVI L3,
- Jumbo frame 9198B,
- 64 połączenia zagregowane typu „port channel”,
- 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP;

Obsługa protokołu NTP,

Obsługa IGMPv1/2/3,

Obsługa standardu IEEE 802.1ae (MACSec) szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,

System operacyjny przełącznika umożliwi wgrywanie poprawek bez konieczności restartowania platformy,

Wsparcie dla funkcjonalność klasyfikowania ruchu w warstwach 4-7 i na jego podstawie budowanie polityk bezpieczeństwa czy jakości usług,

Rozpoznawanie i klasyfikacja około 1400 predefiniowanych znanych aplikacji sieciowych oraz około 150 aplikacji szyfrujących ruch,

System operacyjny przełącznika ma być konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwi eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów,

Wsparcie dla protokołu RESTCONF,

Ma mieć możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia,

Przełącznik realizuje następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

- IEEE 802.1w Rapid Spanning Tree,
- Per-VLAN Rapid Spanning Tree (PVRST+),
- IEEE 802.1s Multi-Instance Spanning Tree,
- Obsługa 256 instancji protokołu STP;

Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED,

Realizacja funkcji 802.1Q tunneling (QinQ),

Funkcja serwera DHCP,

Obsługa 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwi zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,

Obsługa list kontroli dostępu (ACL) następujących typów:

- Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
- VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
- Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
- Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

Przełącznik realizuje następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:

- 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
- Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,
- Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting,
- Kontrola sztormów dla ruchu broadcast/multicast/unicast,

- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

Przełącznik ma posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

Wymagana jest realizacja funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),

Urządzenie realizuje routing statyczny i dynamiczny dla IPv4 i IPv6 ma posiadać w zakresie:

- Routing statyczny dla IPv4 i IPv6,
- Routing dynamiczny dla IPv4: RIP, EIGRP-stub, OSPF, BGP, ISIS, EIGRP (rfc7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA),
- Routing dynamiczny dla IPv6: OSPFv3,
- Funkcjonalności Policy-based routing,
- Multicast routing (PIM-SM, PIM-SSM) ,
- Obsługa protokołu redundancji bramy (VRRP) z obsługą 255 grup,
- Obsługa 100 tuneli GRE (Generic Routing Encapsulation),
- Obsługa 256 wirtualnych instancji routingu (VRF),

Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

Realizacja funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 2000 translacji,

Urządzenie realizuje protokołu LISP zgodnie z RFC 6830,

Urządzenie umożliwi enkapsulację ruchu przy pomocy VXLAN’ów,

Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine,

Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,

Urządzenie ma być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze mają zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,

Klastrowanie ma wspierać funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami,

Przełącznik umożliwi lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

Ma mieć możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),

Ma posiadać funkcjonalność sondy IP SLA (Essential: Responder) do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,

Przełącznik ma posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

Ma posiadać wbudowany analizator pakietów,

Ma posiadać możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:

- Statycznie w oparciu o port, do którego podłączona jest stacja,
- Statycznie w oparciu o VLAN, w którym pracuje stacja,
- Statycznie w oparciu o adres IP stacji,
- Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;

Ma posiadać możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,

Ma posiadać propagację informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa,

Urządzenie umożliwi uruchamianie dodatkowych aplikacji w kontenerach Docker,

Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku M2 SATA o pojemności 240/480/960GB,

MA mieć możliwość realizacji funkcji kontrolera dla radiowych punktów dostępowych WiFi z obsługą do 200 AP oraz 4000 klientów bezprzewodowych,

Urządzenie ma realizować następujące funkcjonalności z zakresu MPLS:

- L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC,
- L2VPN - Virtual Private LAN Services (VPLS) - obsługa 128 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji,
- L3 VPN - MPLS Virtual Private Network (VPN),
- Multicast VPN (MVPN),
- Inter AS Option A i B,
- EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS),
- MPLS over GRE,

Urządzenie ma realizować sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi 128 000,

Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

Urządzenie ma posiadać dedykowany port Ethernet do zarządzania out-of-band,

Ma mieć możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwi kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

Urządzenie ma posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

Urządzenie ma być wyposażone w port konsoli USB,

Urządzenie umożliwi tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,

Przełącznik ma posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia,

Przełącznik ma posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

Ma posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

Ma mieć możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU. Głębokość chassis

urządzenia z wentylatorami i zasilaczami mniejsza niż 60 cm,

Przełącznik musi być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,

Przełącznik ma być wyposażony w następujące moduły interfejsowe SFP / SFP+ pochodzące z oferty producenta przełącznika:

- Gigabit Ethernet 1000Base-T,
- Gigabit Ethernet 1000Base-SX,
- Gigabit Ethernet 1000Base-LX/LH,
- Gigabit Ethernet 1000Base-EX,
- Gigabit Ethernet 1000Base-ZX,
- Gigabit Ethernet 1000Base-BX-D/U,
- 10Gigabit Ethernet 10GBase-SR,
- 10Gigabit Ethernet 10GBase-LR,
- 10Gigabit Ethernet 10GBase-LRM,
- 10Gigabit Ethernet 10GBase-ER,
- 10Gigabit Ethernet 10GBase-ZR,
- 10Gigabit Ethernet 10GBase-BX-D/U,
- 10Gigabit Ethernet typu twinax (SFP+ - SFP+) o długości X metrów;

Przełącznik ma być wyposażony w moduł:

- 8-portowy moduł 10Gigabit Ethernet SFP+
- 2- portowy moduł 40Gigabit Ethernet QSFP

Przełącznik musi posiadać możliwość wyposażenia w następujące moduły QSFP pochodzące z oferty producenta przełącznika:

- 40G-SR4,
- 40G-LR4,
- 40G-ER4,
- 40G-SR-BD,
- 40G-CSR,
- 40G-CSR4,
- 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652),
- adapter 40G QSFP->10G SFP+,
- 40Gigabit Ethernet typu twinax (QSFP - QSFP) o długości X metrów;

Urządzenie ma być wyposażone w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat

Licencja subskrypcyjna oprócz funkcjonalności przełącznika ma obejmować:

- 50 licencji dla systemu kontroli dostępu do sieci,
- 100 licencji na obsługę analizowanych strumieni (flow) dla systemu monitorowania bezpieczeństwa i wykrywania anomalii w sieci;

Minimalne wymagania dla Switch 48 Potrt RJ45 PoE+ (zgodne z IEEE 802.3at), 4x1G

Liczba portów
48 portów 10/100/1000BaseT RJ-45 PoE+ + uplink 4x1G SFP

Moc dostępna dla PoE:
- 740W (z jednym zasilaczem o mocy 1KW),
- 740W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie redundantnym),
- 1440W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie współdzielenia mocy),
- 370W (z jednym zasilaczem o mocy 600W),
- 370W (z dwoma zasilaczami o mocy 600W pracującymi w układzie redundantnym),
- 740W (z dwoma zasilaczami o mocy 600W pracującymi w układzie współdzielenia mocy),

Porty SFP możliwe do obsadzenia następującymi rodzajami wkładek:
- Gigabit Ethernet 1000Base-T,
- Gigabit Ethernet 1000Base-SX,
- Gigabit Ethernet 1000Base-LX/LH,
- Gigabit Ethernet 1000Base-EX,
- Gigabit Ethernet 1000Base-ZX,
- Gigabit Ethernet 1000Base-BX-D/U

Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek
- Gigabit Ethernet 1000Base-T,
- Gigabit Ethernet 1000Base-SX,
- Gigabit Ethernet 1000Base-LX/LH,
- Gigabit Ethernet 1000Base-EX,
- Gigabit Ethernet 1000Base-ZX,
- Gigabit Ethernet 1000Base-BX-D/U,
- 10Gigabit Ethernet 10GBase-SR,
- 10Gigabit Ethernet 10GBase-LR,
- 10Gigabit Ethernet 10GBase-ER,
- 10Gigabit Ethernet 10GBase-ZR,
- 10Gigabit Ethernet typu twinax (SFP+ - SFP+)

Porty SFP/SFP+/SFP28 możliwe do obsadzenia następującymi rodzajami wkładek
- Gigabit Ethernet 1000Base-T,
- Gigabit Ethernet 1000Base-SX,
- Gigabit Ethernet 1000Base-LX/LH,
- Gigabit Ethernet 1000Base-EX,
- Gigabit Ethernet 1000Base-ZX,
- Gigabit Ethernet 1000Base-BX-D/U,
- 10Gigabit Ethernet 10GBase-SR,

- 10Gigabit Ethernet 10GBase-LR,
- 10Gigabit Ethernet 10GBase-ER,
- 10Gigabit Ethernet typu twinax (SFP+ - SFP+),
- 25Gigabit Ethernet 25GBASE-SR,
- 25Gigabit Ethernet typu twinax (SFP28 – SFP28),
- 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),
- 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)

Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
- Przepustowość w ramach stosu - 80Gb/s,
- 8 urządzeń w stosie,
- Zarządzanie poprzez jeden adres IP,
- Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

Zasilanie i chłodzenie:
- Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" – ang. hot swap),
- Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
- W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwi przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),
- Redundantne wentylatory

Parametry wydajnościowe:
- Przepustowość przełącznika (switching capacity):
- 104 Gb/s (bez podłączenia do stosu), 184 Gb/s (z podłączeniem do stosu)
- 176 Gb/s (bez podłączenia do stosu), 256 Gb/s (z podłączeniem do stosu)

Prędkość przesyłania (forwarding rate):
  - 77.38 Mpps
- Bufor pakietów – 6MB
- Pamięć DRAM – 2GB
- Pamięć flash – 4GB
- Obsługa:
  - 500 aktywnych sieci VLAN
  - 16000 adresów MAC
  - 3000 tras IPv4
  - 1500 tras IPv6
  - Ilość wpisów w listach kontroli dostępu Security ACL – 1000
  - ilość wpisów w listach kontroli dostępu QoS ACL – 1000
  - 512 interfejsów SVI L3
  - Jumbo frame 9198B
  - 48 połączeń zagregowanych typu „port channel"
  - 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

Obsługa protokołu NTP

Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

Przełącznik ma wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

- IEEE 802.1w Rapid Spanning Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
- IEEE 802.1s Multi-Instance Spanning Tree
- Obsługa 64 instancji protokołu STP
- Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
- Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku podstawowego

Obsługa protokołu LLDP i LLDP-MED.

Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ)

Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

Możliwość uruchomienia funkcji serwera DHCP

Mechanizmy związane z bezpieczeństwem sieci:

Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

• Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,

• Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

• Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,

• Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,

• Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,

• Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

• Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,

• Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),

• Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,

• Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),

• Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,

• Obsługa list kontroli dostępu (ACL) następujących typów:

- Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
- VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
- Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
- Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);

• Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),

• Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

• Funkcja Private VLAN z obsługą dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS,

• Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci,

Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

•sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,

•bezpieczna sekwencja uruchamiania,

•sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

Mechanizmy związane z zapewnieniem jakości usług w sieci:

• Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,

• Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,

• Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

• Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

• Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

• Kontrola sztormów dla ruchu broadcast/multicast/unicast,

• Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

Obsługa protokołów i mechanizmów routingu:

• Routing statyczny dla IPv4 i IPv6,

• Routing dynamiczny – RIP, OSPF do 1000 routes [Uwaga! w przypadku większej ilości routów jest wymagana licencja Network Advantage / DNA Advantage], PIM Stub do 1000 routes [Uwaga! w przypadku większej ilości routów jest wymagana licencja Network Advantage / DNA Advantage],

• Policy-based routing (PBR),

• Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,

• Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

Przełącznik umożliwi lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

Przełącznik ma posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

Przełącznik ma posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),

Funkcjonalność sondy IP SLA Responder,

Zarządzanie
• Port konsoli,

• Dedykowany port Ethernet do zarządzania out-of-band,

• Ma mieć możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwi kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

• Plik konfiguracyjny urządzenia ma być możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

• Ma mieć obsługę protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

• Ma mieć możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,

• Ma mieć wsparcie dla protokoły RESTCONF,

• Ma mieć wsparcie dla protokołu gNMI,

• Przełącznik ma posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

• Przełącznik ma posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,

• Ma posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

• Ma posiadać funkcję programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

• Ma mieć wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:

I. Monitoring pracy przełącznika w zakresie:

A. Użycie CPU, użycie pamięci, temperatura pracy,

B. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,

C. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,

D. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)

E. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,

F. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,

G. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,

H. Protokół REP (Resilient Ethernet Protocol),

I. Protokół STP (Spanning Tree Protocol),

J. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),

II. Konfigurację przełącznika w zakresie:

A. Konfiguracja interfejsów:

• Fizycznych:

- opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,

- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),

- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,

- przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

• Logicznych typu „port channel":

- opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,

- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,

- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,

- przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

• Wirtualnych typu SVI:

- opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP)

• Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,

• Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),

• Konfiguracja mechanizmów SPAN i RSPAN,

• Konfiguracja protokołu STP,

• Konfiguracja protokołu REP,

• Konfiguracja routingu statycznego i dynamicznego,

• Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,

• Tworzenie i przypisanie list kontroli dostępu ACL,

• Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,

• Konfiguracja i uruchomienie NetFlow,

• Konfiguracja polityk QoS,

• Administracja przełącznika w zakresie:

• Zdalne uruchamianie komend linii poleceń,

• Nazwa przełącznika,

• Tryb pracy L2/L3,

• Adres IP przełącznika do celów zarządzania zdalnego,

• Konfiguracja serwera DHCP,

• Konfiguracja DNS,

• Czas systemowy w tym protokół NTP,

• Konta administracyjne,

• Upgrade oprogramowania,

• Backup konfiguracji,

• Zdalny restart urządzenia,

• Konfiguracja i dostęp przez SNMP,

• Diagnostyka urządzenia:

• Narzędzie PING i TRACEROUTE,

• Przeglądanie logów systemowych,

• Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

Parametry fizyczne:

Możliwość montażu w szafie rack 19”, Wysokość urządzenia 1 RU, Głębokość chassis urządzenia bez wentylatorów i zasilaczy mniejsz niż 30 cm

Głębokość chassis urządzenia z wentylatorami i zasilaczami; mniejsza niż 33 cm

Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwi monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

Wsparcie dla protokołu LISP zgodnie z RFC 6830,

Ma zapewnić obsługę zaawansowanych protokołów routingu:

• IS-IS dla IPv4 i IPv6,

• OSPF,

• EIGRP (rfc7868),

• Routing multicastów - PIM-SM, PIM-SSM,

• Multicast Source Discovery Protocol (MSDP),

Ma mieć możliwość enkapsulacji ruchu w pakiety VXLAN,

Ma zapewnić funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,

Ma mieć możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:

• Statycznie w oparciu o port do którego podłączona jest stacja,

• Statycznie w oparciu o VLAN, w którym pracuje stacja,

• Statycznie w oparciu o adres IP stacji,

• Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;

Ma mieć możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,

Ma zapewnić propagację informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa,

Ma zapewnić współpracę z systemem ochrony opartym o filtrację zapytań DNS (DNS query). Przechwytywanie zapytań DNS i skierowanie ich do systemu analizy danej domeny (FQDN) pod kątem reputacji i bezpieczeństwa,

Przełącznik zapewni widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),

Urządzenie ma być wyposażone w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat,

Przełącznik ma być wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego.

Minimalne wymagania dla Switch przemysłowy 8xRJ45, 4xSFP

• Typ przełącznika - Zarządzany

• Przełącznik wielowarstwowy - L2

- Obsługa jakość serwisu (QoS) - Tak
- Zarządzanie przez stronę www - Tak
- Kształtowanie ruchu – Tak
- Podstawowe przełączanie RJ-45 Liczba portów Ethernet - 8
- Podstawowe przełączania Ethernet RJ-45 porty typ - Fast Ethernet (10/100)
- Ilość portów Fast Ethernet (copper) - 8
- Liczba portów SFP Combo - 2
- Liczba portów USB 2.0 - 1
- Złącze zasilania - DC-in jack
- Standardy komunikacyjne - IEEE 802.3ab,IEEE 802.3u,IEEE 802.3x,IEEE 802.3z
- Obsługa 10G - Nie
- Pełny dupleks - Tak
- Przekierowywanie IP - Tak
- Agregator połączenia - Tak
- Kontrola wzrostu natężenia ruchu - Tak
- Protokół drzewa rozpinającego - Tak
- Obsługa sieci VLAN - Tak
- Liczba VLANs - 255
- Przepustowość - 6,5 Mpps
- Wielkość tabeli adresów - 8000 wejścia
- Pamięci bufora pakietów - 2 MB
- Funkcje DHCP - DHCP server
- Lista kontrolna dostępu (ACL) - Tak
- Szyfrowanie / bezpieczeństwo - FIPS 140-2,SSH-2
- Filtrowanie adresów MAC - Tak
- Obsługuje SSH/SSL - Tak
- Filtrowanie BPDU / Ochrona - Tak
- Obsługa Multicast - Tak
- Liczba grup multiemisji filtrowanych - 255
- Protokoły zarządzające - SNMPv3
- Kolor produktu - Czarny

• Bezpieczeństwo - UL 60950-1, CSA C22.2 No. 60950-1, EN 60950-1, CB IEC 60950-1, NOM NOM-019-SCF1

• Certyfikaty - FCC, IEC/EN 55022A, VCCI, AS/NZS CISPR 22, CISPR 11, CISPR 22, IEC 60068-2-27, IEC 60068-2-6, IEC 60068-2-64, EN 61373, UL/CSA, CE, AS/NZ RCM, BSMI, KCC, ANATEL, RoHS

• Pojemność pamięci wewnętrznej - 256 MB

• Wielkość pamięci flash - 64 MB

• MTBF (Średni okres międzyawaryjny) - 374052 h

• Napięcie wejściowe AC - 110 - 220 V

• Pobór mocy - 15 W

• Obsługa PoE - Nie

• Zakres temperatur (eksploatacja) - -40 - 70 °C

• Zakres temperatur (przechowywanie) - -40 - 85 °C

• Dopuszczalna wilgotność względna - 5 - 95%

• Dopuszczalna wysokość podczas eksploatacji (n.p.m.) - 0 - 4572 m

• Dopuszczalna wysokość (n.p.m.) - 0 - 4572 m

• Szerokość produktu - 88,9 mm

• Głębokość produktu - 133,6 mm

• Wysokość produktu - 127 mm

UWAGI OGÓLNE

Kompleksowa platforma bezpieczeństwa składająca się minimum z:

- Systemu Kontroli Dostępu – zgodnego z grade 4 według normy EN60839, potwierdzonego certyfikaty wydane przez zewnętrzną uprawnioną jednostkę certyfikującą.
- Systemu Sygnalizacji Włamania i Napadu zgodny z grade 3 według normy EN50131

System musi się cechować następującymi funkcjonalnościami w zakresie bezpieczeństwa:

- Komunikacja z wykorzystaniem protokołu TCP/IP w systemie jest szyfrowana i zabezpieczona protokołem SSL/TLS w wersji 1.3.
- System musi pozwalać na import certyfikatów SSL przygotowanych przez klienta i podpisanych przez podmiot, który wystawia zaufane certyfikaty cyfrowe (ang. Certificate Authority, CA). Nie dopuszcza się stosowania certyfikatów dostarczonych przez producenta systemu kontroli dostępu.