

Minimalne wymagania równoważne parametrów technicznych systemów Zabezpieczenia Technicznego dopuszczone dla Systemu CCTV, Archiwizacji Danych, VMS (Video Management System), Warstwy Aktywnej, Sieci Okablowania LAN oraz Systemu Zarządzania Bezpieczeństwem. W przypadku pozostałych elementów wyspecyfikowanych w SWZ zał. nr 8 to jest; System Kontroli dostępu, Systemu Sygnalizacji Włamania i Napadu należy zastosować rozwiązania przewidziane w SWZ zał. Nr 8.

1. Minimalne parametry techniczne dla Systemu Zarządzania Bezpieczeństwem

- System zarządzania musi być niezależny od producentów integrowanych rozwiązań. PSIM musi mieć zdolność integrowania dowolnych systemów za pomocą dowolnych protokołów komunikacyjnych
- Wymagane się aby system PSIM zapewnił dwukierunkową łączność podsystemami. Musi zostać zapewniona możliwość sterowania zintegrowanymi systemami np. nadawanie uprawnień w systemie kontroli dostępu, blokowanie czujek systemu ppoż, sterowanie kamerami.
- Wymagane jest aby system PSIM umożliwiał wymianę informacji z użytkownikami mobilnymi opartymi o urządzenia GSM/GPS
- Oprogramowanie musi być zbudowane w sposób modułowy. Modernizacja lub wymiana dowolnego modułu programowego nie może wstrzymywać pracy pozostałych modułów i funkcji systemu
- PSIM musi być administrowany i obsługiwany w pełni przez przeglądarkę internetową. Nie dopuszcza się stosowania dedykowanej aplikacji instalowanej na stacji roboczej
- Wymagana jest możliwość pomiaru wielkości fizycznych typu ciągłego (np. prąd ładowania baterii, wartość napięcia, temperatury, ciśnienia itp.) z wymaganą częstotliwością nie mniejszą niż 1 pomiar na sekundę. Wymagana jest możliwość generowania alarmów na podstawie przekroczenia progów alarmowych
- Wymagane jest aby system PSIM automatycznie powracał do stanu pracy. Niezbędne składniki oprogramowania (moduły) muszą być uruchamiane automatycznie (np. usługi systemu operacyjnego).
- System PSIM musi posiadać 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 zależności od działań podjętych przez operatora.
- Wymagane jest aby system PSIM posiadał możliwość załączania dowolnych dokumentów cyfrowych przypisanych do konkretnych procedur działania, czujników lub urządzeń.
- System musi zapewnić mechanizm swobodnego kształtowania układu ramek aplikacji tak, aby dowolna zawartość mogła być zagnieżdżana np. w układzie siatki.
- PSIM musi zapewnić moduł wprowadzania adresów i kontaktów - baza serwisantów, pojazdów itp.
- Instalacja PSIM musi być zabezpieczona bezpiecznym połączeniem z serwerem za pomocą SSL.
- Wymagane jest, aby system PSIM musiał pracować w architekturze zorientowanej na usługi (ang. SOA).
- 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.
- Wymaga się aby system PSIM posiadał aktualny certyfikat i świadectwo dopuszczenia CNBOP do dwukierunkowej komunikacji z urządzeniami przeciwpożarowymi,
- Wymagana jest sygnalizacja przerwy komunikacji z każdym integrowanym systemem poprzez wyświetlenie odpowiedniego komunikatu alarmowego.
- Wymagane jest aby system posiadał możliwość podłączenia dowolnego urządzenia lub systemu za pomocą protokołu komunikacyjnego

- PSIM musi umożliwiać odbiór i transmisję informacji i zdarzeń do i z urządzeń związanych z niniejszym projektem. Pozwoli to na pełne zdalne sterowanie wszelkimi urządzeniami i/lub systemami zarządzanymi przez PSIM. Platforma PSIM musi umożliwiać sprawne współdziałanie pomiędzy podsystemami bezpieczeństwa
- Rozwiązanie PSIM musi zapewniać mechanizm wywołania, który pozwala na reakcję PSIM na zdarzenia mające miejsce w dowolnym obiekcie będącym pod kontrolą PSIM. W Uzgodnieniu ze Zleceniodawcą należy dostarczyć opisy scenariuszy alarmowych, aby umożliwić tworzenie bardziej złożonych warunków alarmu, obejmujących logiczne porównanie różnych obiektów wywołujących.
- System musi pozwalać na kontrolę podsystemów, takich jak np. kontrola dostępu, aby umożliwić przejście funkcji zezwolenia na dostęp. W takim przypadku spowoduje to również podniesienie systemu PSIM do rangi nadzorującego pod określonymi na etapie konfiguracji warunkami,
- System poprzez integrację z systemem kontroli dostępu KD i systemem sygnalizacji włamania i napadu SWIN musi zapewnić możliwość zliczania ludzi w miejscach zbiórki do ewakuacji oraz zliczać ilość osób przebywających w pomieszczeniach. System poprzez integrację z SAP powinien zapewnić możliwość blokowania i testowania elementów,
- Wymagane jest, aby system PSIM posiadał możliwość tworzenia raportów dziennych, miesięcznych, kwartalnych ze sprawności integrowanych systemów.

2. Minimalne parametry techniczne dla urządzeń aktywnych

2.1 Switch 48port

- Typ przełącznika - Zarządzany
- Obsługa jakości serwisu (QoS) – Tak
- Zarządzanie przez stronę www - Tak
- Podstawowe przełączanie RJ-45 Liczba portów Ethernet - 48
- Podstawowe przełączania Ethernet RJ-45 porty typ - Gigabit Ethernet (10/100/1000)
- Liczba zainstalowanych modułów SFP - 2
- Liczba zainstalowanych modułów SFP+ - 2
- Liczba portów USB 2.0 - 3
- Standardy komunikacyjne - IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3at, IEEE 802.3bz, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z
- Obsługa 10G - Tak
- Technologia okablowania Copper Ethernet - 100BASE-FX, 1000BASE-LX, 1000BASE-SX, 1000BASE-T
- Przekierowywanie IP - Tak
- Pozycja routingu - 3000
- Protokół drzewa rozpinającego - Tak
- Technologie wirtualizacji sieci - Virtual Extensible LAN (VXLAN)
- Trasy IPv4 - 3000
- Trasy IPv6 - 1500
- Liczba VLANs – 1024
- Przepustowość routowania/przełączania - 176 Gbit/s
- Prędkość przekazywania - 130,95 Mpps
- Wielkość tabeli adresów - 16000 wejścia
- Zgodny z Jumbo Frames - Tak
- Rozszerzenie Jumbo Frames - 9198
- Pamięci bufora pakietów - 6 MB
- Lista kontrolna dostępu (ACL) - Tak
- Szyfrowanie / bezpieczeństwo - 128-bit AES
- Obsługa Multicast - Tak
- Protokoły zarządzające - SNMPv1/v2c/v3
- Protokół wybierania drogi - CDP, EIGRP, OSPF, RIP, VRRP
- Produkt stackowalny - Tak

- Kolor produktu - Szary
- Bezpieczeństwo - IEC 60950-1, UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1, AS/NZS 60950.1, Class I Equipment
- Standardy EMC - 47 CFR Part 15, CISPR 22 Class A, CISPR 32 Class A, CNS 13438, EN 300 386, EN 55022 Class A, EN 55032 Class A, EN61000-3-2, EN61000-3-3, ICES-003 Class A, KN 32, TCVN 7189 Class A, V-3 Class A, CISPR 24, EN 300 386, EN 55024, KN 35, TCVN 7317
- Certyfikaty - RoHS
- Typ pamięci - DRAM
- Pojemność pamięci wewnętrznej - 2048 MB
- Wielkość pamięci flash - 4096 MB
- Poziom hałasu - 42 dB
- Obsługa funkcji Plug & Play - Tak
- MTBF (Średni okres międzyawaryjny) - 346270 h
- Zasilacz dołączony - Tak
- Obsługa zasilania zapasowego (RPS) - Tak
- Napięcie wejściowe AC - 100 - 240 V
- Częstotliwość wejściowa AC - 50 - 60 Hz
- Prąd wejściowy - 6 - 12 A
- Obsługa PoE - Tak
- Power over Ethernet Plus (PoE +) ilość portów - 48
- Zasilanie przez Ethernet (PoE) zasilanie na port - 30 W
- Całkowita Power over Ethernet (PoE) budżetu - 740 W
- Zakres temperatur (eksploatacja) - -5 - 45 °C
- Zakres temperatur (przechowywanie) - -40 - 70 °C
- Zakres wilgotności względnej - 5 - 90%
- Dopuszczalna wysokość podczas eksploatacji (n.p.m.) - 0 - 3000 m
- Emisja ciepła - 3412 BTU/h
- Szerokość produktu - 445 mm
- Głębokość produktu - 329 mm
- Wysokość produktu - 44 mm

2.2 Switch 16 port SFP

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

- Przełącznik posiada jeden dodatkowy slot na moduł rozszerzeń. Dostępne są następujące moduły:
- 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 umożliwiają 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 jest wyposażone w wymienne moduły wentylatorów,
 - Urządzenie może zostać wyposażone w zasilacz redundantny do pracy w trybie 1:1;
 - Urządzenie posiada 32MB bufor pamięci,
 - 16GB pamięci DRAM i 16GB pamięci flash,
 - Przepustowość przełącznika (switching capacity) wynosi 480 Gbps,
-
- 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 umożliwia wgrzywanie poprawek bez konieczności restartowania platformy,
 - Wsparcie dla funkcjonalności 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 jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modeli danych YANG (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów,
 - Wsparcie dla protokołu RESTCONF,
 - Możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia,
 - 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 umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią 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 samej 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 szturmów 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 posiada wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
- 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 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 umożliwia 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 jest przygotowane sprzętowo do łączenia w klastrer z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze będą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,

- Klastrowanie wspiera funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klastery pomiędzy przełącznikami,
- Przełącznik umożliwia 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,
- 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),
- 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 posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowania zewnętrznego,
- Wbudowany analizator pakietów,
- 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;
- Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
- Propagacja 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 umożliwia 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,
- Możliwość realizacji funkcji kontrolera dla radiowych punktów dostępowych WiFi z obsługą do 200 AP oraz 4000 klientów bezprzewodowych.

Urządzenie realizuje 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 obsługą MACSec (MACsec over EoMPLS),
- MPLS over GRE,

Zarządzanie i konfiguracja:

- Urządzenie realizuje 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 posiada dedykowany port Ethernet do zarządzania out-of-band,
- 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 umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

- Urządzenie posiada port USB umożliwiający podłączenie zewnętrznego nośnika danych.
- Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
- Urządzenie jest wyposażone w port konsoli USB,
- Urządzenie umożliwia 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 posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia,
- Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
- Funkcja 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,
- Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU. Głębokość chassis urządzenia z wentylatorami i zasilaczami mniejsza niż 60 cm, ,

2.3 Switch przemysłowy 8port RJ45,2xSFP

- Typ przełącznika - Zarządzany
- Przełącznik wielowarstwowy - L2
- Obsługa jakości 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 duplex - 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

3. Minimalne wymagania dla kamer

3.1 Wymagane parametry kamery stałopozycyjnej tubowej (typu bullet)

- przetwornik obrazu: CMOS formatu co najmniej 1/3" ze skanowaniem progresywnym
- liczba aktywnych pikseli nie mniej niż 2688 (H) x 1520 (V)
- szybkość przetwarzania obrazu do 30 kl/s włącznie dla pełnej rozdzielczości
- kompresja obrazu: H.264 i H.265
- generowanie co najmniej 3 strumieni wideo
- tryby pracy dziennej i nocnej (filtr ICR)
- szeroki zakres dynamiczny (True WDR) minimum 120dB
- minimalne natężenie światła: 0,005 lux lub mniej w trybie kolorowym (dla F1.5 i 30IRE), 0,0005 lux lub mniej w trybie monochromatycznym (dla F1.5 i 30IRE) bez włączonego oświetlacza IR i 0 lux w trybie monochromatycznym przy włączonym oświetlaczu IR
- obiektyw zintegrowany z funkcjami moto-zoom i autofocus o ogniskowej w zakresie od 2,7mm do 13,5mm lub szerszym
- automatyczne i ręczne sterowanie czasem ekspozycji
- automatyczna i ręczna regulacja balansu bieli
- detekcja ruchu
- wbudowana analityka wideo z co najmniej następującymi funkcjami: detekcja intruza (przekroczenia wirtualnej linii i wejścia w wirtualny obszar) z klasyfikacją obiektów typu „człowiek” i „pojazd”
- możliwość zdefiniowania co najmniej 4 stref prywatności
- standard interfejsu sieciowego: 100BASE-TX
- wbudowane gniazdo na kartę SD lub micro SD o pojemności do 256GB włącznie
- wejście i wyjście audio
- co najmniej jedno wejście i jedno wyjście alarmowe
- zintegrowana obudowa typu bullet o klasie szczelności IP67
- zintegrowany oświetlacz podczerwieni (IR) o zasięgu 60 metrów
- zasilanie 12VDC i PoE+ (IEEE802.3at) lub PoE (IEEE802.3af)

- zgodność ze standardem ONVIF
- możliwość pracy w zakresie temperatur od -30 st. C. do +60 st. C. lub szerszym

3.2 Wymagane parametry kamery stałopozycyjnej kopułowej

- przetwornik obrazu: CMOS formatu co najmniej 1/3" ze skanowaniem progresywnym
- liczba aktywnych pikseli nie mniej niż 2688 (H) x 1520 (V)
- szybkość przetwarzania obrazu do 30 kl/s włącznie dla pełnej rozdzielczości
- kompresja obrazu: H.264 i H.265
- generowanie co najmniej 3 strumieni wideo
- tryby pracy dziennej i nocnej (filtr ICR)
- szeroki zakres dynamiczny (True WDR) minimum 120dB
- minimalne natężenie światła: 0,005 lux lub mniej w trybie kolorowym (dla F1.5) i 0 lux w trybie monochromatycznym przy włączonym oświetlaczu IR
- obiektyw zintegrowany z funkcjami moto-zoom i autofocus o ogniskowej w zakresie od 2,7mm do 13,5mm lub szerszym
- automatyczne i ręczne sterowanie czasem ekspozycji
- automatyczna i ręczna regulacja balansu bieli
- detekcja ruchu
- wbudowana analityka wideo z co najmniej następującymi funkcjami: detekcja intruza (przekroczenia wirtualnej linii i wejścia w wirtualny obszar) z klasyfikacją obiektów typu „człowiek” i „pojazd”
- możliwość zdefiniowania co najmniej 4 stref prywatności
- standard interfejsu sieciowego: 100BASE-TX
- wbudowane gniazdo na kartę SD lub micro SD o pojemności do 256GB włącznie
- wbudowany mikrofon
- zintegrowana obudowa kopułowa lub typu eyeball o klasie szczelności IP67
- zintegrowany oświetlacz podczerwieni (IR) o zasięgu 40 metrów
- zasilanie 12VDC i PoE+ (IEEE802.3at) lub PoE (IEEE802.3af)
- zgodność ze standardem ONVIF
- możliwość pracy w zakresie temperatur od -30 st. C. do +60 st. C. lub szerszym

3.3 Wymagane parametry kamery obrotowej (PTZ)

- przetwornik obrazu: CMOS formatu 1/2.8" ze skanowaniem progresywnym
- liczba aktywnych pikseli nie mniej niż 2560 (H) x 1440 (V)
- szybkość przetwarzania obrazu do 30 klatek/s przy pełnej rozdzielczości
- obsługiwana kompresja obrazu: H.264 i H.265
- generowanie co najmniej 3 strumieni wideo
- tryby pracy dziennej i nocnej (filtr ICR)
- szeroki zakres dynamiczny (WDR) minimum 120dB
- minimalne natężenie światła: 0,005 lux lub mniej w trybie kolorowym (dla F1.6), 0,0005 lux lub mniej w trybie monochromatycznym (dla F1.6) bez włączonego oświetlacza IR i 0 lux w trybie monochromatycznym przy włączonym oświetlaczu IR
- obiektyw zintegrowany o ogniskowej w zakresie od 4 mm do 177 mm lub szerszym
- wbudowany reflektor podczerwieni o zasięgu do 150 metrów włącznie
- zoom cyfrowy co najmniej 16x
- funkcje moto-zoom i autofocus
- kompensacja oświetlenia tła: BLC / HLC
- automatyczna i ręczna regulacja balansu bieli
- standard interfejsu sieciowego: 100BASE-TX
- wbudowany slot na kartę micro-SD
- wejście i wyjście audio
- co najmniej dwa wejścia i jedno wyjście alarmowe

- detekcja ruchu
- wbudowana analityka wideo z co najmniej następującymi funkcjami: detekcja intruza (przekroczenia wirtualnej linii i wejścia w wirtualny obszar) z klasyfikacją obiektów typu „człowiek” i „pojazd”
- możliwość tworzenia do 24 stref prywatności włącznie
- możliwość zdefiniowania 300 presetów i 8 tras patrolowych
- zakres obrotu: w poziomie 360 stopni (bez ograniczeń), w pionie od -15 do 90 stopni
- prędkość obrotu w poziomie (pan): od 0.1-300 stopni / sek. w sterowaniu ręcznym i 400 stopni / sek. dla presetów
- prędkość obrotu w pionie (tilt): od 0.1-200 stopni / sek. w sterowaniu ręcznym i 300 stopni / sek. dla presetów
- zasilanie 24VAC i PoE+ (IEEE802.3at)
- zgodność ze standardem ONVIF
- klasa szczelności IP67
- stopień wandaloodporności IK10
- praca w zakresie temperatur od -40 st. C. do +60 st. C.. lub szerszym

4. Minimalne wymagania dla oprogramowania zarządzającego kamerami (VMS)

- Oprogramowanie musi posiadać czytelną, prostą politykę licencjonowania opartą o klucze licencyjne z możliwością ich grupowania w celu optymalizacji kosztowej dla użytkowników końcowych;
- Oprogramowanie musi opierać się o licencjonowanie dostępu (możliwości podłączenia) kamer wideo lub innych źródeł wideo o specyfikacji szczegółowo opisanej w dalszej części wymagań;
- Oprogramowanie musi być skalowalne od jednego klienta, serwera i kamery do setek klientów, serwerów i kamer;
- Oprogramowanie musi posiadać elastyczną, skalowalną – co najmniej 3 stopniową skalę (wersję) funkcjonalności oprogramowania z możliwością migracji do wyższej wersji z niższej (mniejszej liczby funkcjonalności);
- Oprogramowanie musi udostępniać nieodpłatną aplikację kliencką bez ograniczeń ilościowych w instalacji w zakresie urządzeń – stacji oglądowych;
- Oprogramowanie musi udostępniać pakiet API/SDK w celu integracji z rozwiązaniami trzecimi;
- Oprogramowanie musi udostępniać nieodpłatną wersję oprogramowania dla aplikacji mobilnych z obsługą urządzeń opartych co najmniej o system iOS i Android;
- Rozbudowa systemu musi być możliwa w każdej chwili nawet o pojedynczą kamerę (licencję);
- Licencje muszą fluktuować w ramach danej grupy serwerów tworzących dany system tj. nie mogą być przydzielone do konkretnego serwera, a muszą być dedykowane dla całej instalacji (jako jednego obiektu).

Podstawowe wymagania dla aplikacji serwerowej

- Aplikacja serwerowa nie może być ograniczona pod względem producenta sprzętu na którym ma pracować, a jedynie parametrami technicznymi i wydajnościowymi umożliwiającymi jej poprawne, płynne i nieprzerwane wykorzystanie;
- Praca w architekturze klient-serwer, w tym wiele serwerów i jeden klient oraz wiele serwerów i wiele stacji klienckich, a w ramach jednego systemu do najmniej 25 000 kamer i co najmniej 100 serwerów;
- Otwarta architektura klient-serwer pozwalająca na podłączenie do systemu Nielimitowanej liczby nowych urządzeń;
- Możliwość grupowania serwerów w klastry w ramach jednej „logicznej” lokalizacji jako jeden system lub podsystem
- Oprogramowania serwera i klienta muszą posiadać możliwość instalacji i uruchamiania na jednej, wspólnej maszynie, jak również na oddzielnych maszynach;
- Możliwość nagrywania obrazu z co najmniej 250 kamer na jednym serwerze;
- Wsparcie dla kamer sieciowych obsługujących powszechnie stosowane kompresje MJPEG, JPEG2000, MPEG4, H.264, H.265;
- Obsługa kamer wysokich rozdzielczości (kamer megapikselowych) do 40 Mpix włącznie;

- Obsługa kamer producentów trzecich w oparciu o standard ONVIF oraz ewentualne natywne integracje;
- Obsługa kamer multisensorycznych – wieloprzetwornikowych;
- Oprogramowanie musi zapewniać szybkość nagrywania do 100 klatek na sekundę (z jednej kamery) łącznie;
- Oprogramowanie musi zapewniać możliwość grupowania wszystkich serwerów w celu zapewnienia ciągłości pracy systemu na wypadek awarii któregoś z nich – dane o użytkownikach, ich aktywności zdarzeniach, alarmach pozostają niezmienione, nie ulegają utracie w sytuacji awarii któregoś serwera w sieci – grupie (klastrze);
- Ustawienia rejestracji z indywidualnie (dla każdej rejestrowanej kamery) dobranymi parametrami zapisu;
- Ustawienia parametrów rejestracji: ilość klatek/s, rozdzielczość, jakość kompresji przynajmniej 10 poziomów kompresji w tym wizualnie bezstratną;
- Oprogramowanie musi zapewnić opcję nagrywania „buforowego” przed zdarzeniem i nagrywania po zdarzeniu;
- Oprogramowanie musi zapewnić opcję zapisu ramki referencyjnej w przypadku braku zdarzeń w polu widzenia kamery;
- Oprogramowanie musi zapewnić możliwość planowania kopii zapasowych z nagraniami wideo i zdarzeń do folderu lokalnego lub na zmapowany dysk sieciowy;
- Oprogramowanie musi posiadać możliwość automatycznego kasowania najstarszych kopii zapasowych w przypadku wyczerpania się miejsca do zapisu nowych kopii zapasowych.
- Oprogramowanie musi posiadać możliwość rejestracji strumieni audio i wideo w oparciu o harmonogram nagrywania, który można określić indywidualnie dla każdego źródła wideo. Harmonogram musi zawierać obsługę następujących parametrów: szablon nagrywania, nagrywanie ciągle, nagrywanie wykorzystujące detekcję ruchu, nagrywanie zdarzeń aktywacji wejść cyfrowych, nagrywanie zdarzeń alarmowych, nagrywanie zdarzeń transakcji POS, nagrywanie zdarzeń rozpoznania numerów rejestracyjnych, kalendarz dobowy i tygodniowy;
- Możliwość zaimplementowania narzędzi (algorytmów) inteligentnej analizy obrazu (np. rozpoznawania tablic rejestracyjnych, analiza ruchu osób i pojazdów);
- Oprogramowanie musi zapewnić możliwość planowania kopii zapasowych z nagraniami wideo i zdarzeń do folderu lokalnego lub na zmapowany dysk sieciowy;
- Oprogramowanie musi umożliwiać nagrywanie pierwszego lub drugiego lub trzeciego strumienia wideo z danego źródła wideo;
- Oprogramowanie musi umożliwiać wysyłanie do aplikacji klienckiej drugiego strumienia w sytuacji wyświetlania obrazu wideo w podziale większym niż 1x1 w celu optymalizacji pasma transmisji pomiędzy aplikacją serwerową i kliencką;
- Oprogramowanie musi być dostępne w co najmniej następujących językach : polski, angielski, francuski, niemiecki, rosyjski, czeski;
- System nie może mieć ograniczeń pojemności zapisu i musi pozwalać na rozbudowę pojemności zapisu do co najmniej 2000 TB;
- Oprogramowanie musi umożliwiać aktualizację do najnowszej wersji bez konieczności odinstalowywania poprzedniej wersji;
- Aplikacja kliencka musi automatycznie wykrywać wszystkie aplikacje serwerowe uruchomione na komputerach podłączonych do tej samej sieci;
- Oprogramowanie musi mieć funkcję wyszukiwania serwerów uruchomionych na komputerach połączonych w innym segmencie sieci niż klient, za pomocą adresów IP lub nazw hostów;
- Oprogramowanie musi zapewniać jednoczesną archiwizację obrazu i jego odtwarzanie na wielu stanowiskach oglądowych w tym samym czasie;
- Oprogramowanie musi zapewnić możliwość ustawienia limitu maksymalnego pasma dla danych przesyłanych z aplikacji serwerowej do aplikacji klienckiej;
- Oprogramowanie musi zapewniać możliwość aktualizacji jednocześnie wszystkich serwerów pracujących w danej sieci z poziomu stacji klienckiej o uprawnieniach administracyjnych;
- Oprogramowanie musi zawierać usługę, która pozwala podłączyć urządzenia mobilne do systemu. Mobilna aplikacja kliencka musi być obsługiwana przez urządzenia mobilne z systemami Android i iOS

(Apple);

- Mobilna aplikacja kliencka musi obsługiwać powiadomienia typu „push” generowane przez system i analizę wideo;
- Oprogramowanie musi zapewnić możliwość automatycznego logowania się użytkownika do grupy serwerów (klastra);
- Oprogramowanie musi zapewniać możliwość automatycznego wylogowania użytkownika z grupy serwerów (klastra), gdy aplikacja kliencka nie jest używana przez zdefiniowany czas;

Funkcjonalności wspomagające zarządzanie systemem

- Oprogramowanie musi posiadać dedykowaną aplikację do automatycznej (odroczonej) archiwizacji (backup'u) danych wideo z wybranych kamer. Musi istnieć możliwość wyboru przedziału czasowego (z dokładnością do 1 sekundy) archiwizowanego materiału, czasu uruchomienia automatycznej archiwizacji (z dokładnością do 1 sekundy);
- Oprogramowanie musi posiadać dedykowaną aplikację do kasowania automatycznie zatwierdzonych (auto-acknowledged) alarmów. Po skasowaniu alarmów tego typu nadal musi istnieć możliwość ich późniejszego wyszukania i odtworzenia w systemie.
- Oprogramowanie musi posiadać dedykowaną aplikację do monitorowania liczby zakładek (tzw. „Bookmark”) i kasowania wszystkich starszych niż podana data.
- Oprogramowanie musi posiadać dedykowaną aplikację do zarządzania treścią wyświetlaną na wybranych kamerach. Treść musi być wyświetlana w postaci OSD (on screen display) na wszystkich kamerach ze zdefiniowanej grupy jednocześnie.
- Oprogramowanie musi posiadać dedykowaną aplikację do automatycznego (według ustalonego harmonogramu) pobierania logów bezpośrednio z wybranych kamer.

Szczegółowe funkcjonalności aplikacji serwerowej

- Oprogramowanie musi zapewniać kolaboracyjną współpracę niezależnych operatorów systemu poprzez możliwość przekazania przez jednego operatora oglądanych przez niego widoków z kamer (zarówno wyświetlanym na żywo, jak odtwarzanych za nagrań) innym operatorom w czasie rzeczywistym w celu szybszej analizy tych samych kluczowych zdarzeń z kamer przez kilku operatorów;
- System musi mieć możliwość rozbudowy o opcjonalny, w pełni integralny moduł rozpoznawania tablic rejestracyjnych (LPR, ANPR);
- Oprogramowanie musi posiadać możliwość przekazania informacji z tego samego alarmu wielu operatorom systemu wraz z ewentualną eskalacją zdarzeń;
- System musi posiadać funkcjonalność umożliwiającą jednoczesną rejestrację co najmniej dwóch strumieni wideo z tej samej kamery. Administrator musi mieć możliwość zdefiniowania okresu przechowywania podstawowego strumienia, tak, aby strumień ten został usunięty po określonym czasie a strumień dodatkowy pozostawał do końca żądanego okresu przechowywania.;
- System musi posiadać funkcjonalność umożliwiającą automatyczne zmniejszenie poklatkowości do $\frac{1}{2}$ lub $\frac{1}{4}$ zarejestrowanego obrazu wideo w kompresji JPEG2000 i MJPEG w celu optymalizacji czasu przechowywania nagranego materiału wideo;
- Oprogramowanie do zarządzania wideo w sieci musi zapewniać zarządzanie i synchronizację serwerów w obszarze (site) ze współdzielonymi i rozproszonymi danymi konfiguracyjnymi oraz ustawieniami systemu, tak, aby awaria dowolnego serwera nie powodowała utraty tych danych i ustawień systemu;
- Oprogramowanie musi posiadać możliwość przesyłania tylko wybranych fragmentów obrazu pomiędzy serwerami rejestrującymi a stacjami operatorskimi w celu optymalizacji dostępnego pasma z zastrzeżeniem rejestracji na serwerach zapisu obrazów z najlepszą dostępną jakością;
- Oprogramowanie musi posiadać możliwość półautomatycznej aktualizacji całego systemu, czyli wszystkich serwerów i stacji klienckich do najnowszej dostępnej wersji;
- Oprogramowanie musi posiadać funkcję wyszukiwania konkretnych osób w zarejestrowanym materiale wideo (pod warunkiem zastosowania odpowiednich do tego celu kamer lub dedykowanych urządzeń zintegrowanych z VMS). Wyszukiwanie to nie może się ograniczać do jednego serwera i jednej kamery (musi działać na grupie/klastrze serwerów i wielu kamerach podłączonych do różnych

serwerów) i musi polegać co najmniej na:

- kliknięciu przez operatora na postaci poszukiwanej osoby w zarejestrowanym materiale wideo;
- automatycznym zaznaczeniu przez oprogramowanie prawdopodobnych pojawień się tej osoby w postaci znaczników na osi czasu;
- automatycznej prezentacji przez oprogramowanie prawdopodobnych pojawień się tej osoby w postaci miniatur.
- Oprogramowanie musi posiadać funkcję wyszukiwania konkretnych osób w zarejestrowanym materiale wideo (pod warunkiem zastosowania odpowiednich do tego celu kamer lub dedykowanych urządzeń zintegrowanych z VMS) na podstawie cech wyglądu, np. koloru ubrania.

Funkcjonalności aplikacji klienckiej

- Panel główny aplikacji klienckiej musi być konfigurowalny w zakresie co najmniej: wyświetlanych źródeł wideo, map, zdarzeń alarmowych, zapisanych widoków;
- Panel główny musi posiadać z lewej strony czytelne i przejrzyste drzewo katalogowe pozwalające na jego konfigurację w zakresie typów wyświetlanych urządzeń, serwerów, widoków, lokalizacji;
- Panel główny aplikacji klienckiej musi umożliwiać dostęp za pomocą pojedynczego kliknięcia do materiału wideo w trybie „na żywo” i „nagranego”;
- Panel główny musi umożliwiać wyszukiwanie pojedynczych zasobów do których danych użytkownik ma dostęp, co najmniej takich jak: dany serwer, dana mapa, dana kamera, dany widok wideo, dana strona web;
- Panel główny musi posiadać co najmniej poniższe elementy do obsługi wideo:
 - o kursor myszy do wyboru danego serwera, danej kamery, mapy, danego widoku wideo, danej strony web, czy innej akcji jaką użytkownik chce wywołać;
 - o przyciski zoomu cyfrowego „in plus” i „in minus”
 - o przycisk do pracy na przybliżonym materiale wideo
 - o przyciski do sterowania PTZ
 - o przycisk do wyboru układu wyświetlania obrazów wideo i innych źródeł danych
 - o przycisk maksymalizacji danego źródła danych lecz nie mniej niż obrazu z kamery i mapy
 - o przycisk przełączania pomiędzy widokami z kamer
 - o przycisk zapisu danego widoku z kamer
 - o przycisk przesłania danego widoku do innego operatora – funkcja współpracy operatorów
- Dostęp do widoku z danego zasobu z panelu wideo musi odbywać się zarówno poprzez dwukrotny klik lewego przycisku myszki jak i poprzez funkcję „przenieś i upuść”;
- Panel główny musi posiadać narzędzie do wyświetlania kluczowych informacji dla użytkownika wraz z co najmniej 2 kolorową skalowalnością istotności informacji;
- Panel główny aplikacji musi posiadać możliwość minimalizacji okna, maksymalizacji i zamknięcia aplikacji klienckiej;
- Panel główny aplikacji musi umożliwiać pracę opartą o zakładki zawierające widoki z wybranych przez użytkownika kamer czy innych źródeł informacji, przy czym użytkownik musi posiadać pełnię możliwości kreowania informacji w każdej zakładce w ramach posiadanych uprawnień;
- Panel główny musi umożliwiać otwarcie co najmniej 20 różnych zakładek zawierających co najmniej wszystkie poniższe dane:
 - o Widok (logowanie do danej lokalizacji, nowy widok, alarmy i zarządzanie nimi);
 - o Wyszukiwanie zdarzeń (zdarzenie takie jak: ruch, wejście cyfrowe, obiekty sklasyfikowane, miniatury, zdarzenia alarmowe, transakcje POS, zakładki „bookmark”);
 - o Eksport (eksport materiału i archiwizacja);
 - o Zarządzanie (konfiguracja witryny, dziennik witryny);
- Panel główny musi posiadać przycisk do konfiguracji aplikacji klienckiej;
- Panel główny musi posiadać w trybie oglądu materiału nagranego oś czasu z wyświetlaniem co najmniej poniższych informacji: materiał nagrany ciągle, materiał z występowaniem ruchu, dokładna data materiału wideo, informacja o oglądanej kamerze i kamerach (jednoczesny ogląd);
- Panel główny musi mieć możliwość odtwarzania materiału wideo w trybie prędkości od -8x do+8x wraz z prędkościami cząstkowymi -1/4, -1/2, 1/2, 1/4;
- Oprogramowanie musi umożliwiać tworzenie zakładek na nagraniach wideo i audio z wielu źródeł,

wyświetlanie zakładek na osi czasu, i opcję wyszukiwania zakładek;

- Oprogramowanie musi umożliwiać ochronę zakładek tak, aby dane wideo i audio nie były nadpisywane;
- Oprogramowanie musi umożliwiać przeszukiwanie zakładek na podstawie różnych kryteriów, w tym nazwy zakładek, notatek i powiązanych nazw kamer;
- Oprogramowanie musi umożliwiać tworzenie, edycję i usuwanie zakładek „bookmark” przez operatorów (klientów) pracujących w oparciu o klienta sieciowego HTML;
- Panel główny musi posiadać możliwość automatycznego, cyklicznego przełączania pomiędzy otwartymi zakładkami wideo.

Konfiguracja panelu głównego

- Przycisk do konfiguracji panelu głównego musi umożliwiać dostęp do co najmniej: konfiguracji aplikacji klienckiej, instrukcji obsługi, otwarcia nowego okna, zalogowanie się, wylogowanie się, wygenerowanie raportu błędów;
- W ramach konfiguracji aplikacji klienckiej muszą być dostępne co najmniej poniższe funkcje: wyświetlanie powiadomień, synchronizacja odtwarzanego materiału wideo, wybór języka aplikacji klienckiej, automatyczne logowanie do witryny z opcją uwierzytelniania Windows oraz poprzez wpisanie loginu i hasła, zdefiniowanie pasma pomiędzy klientem i serwerem;
- W ramach konfiguracji aplikacji klienckiej musi istnieć możliwość tworzenia nakładek obrazu takich jak: nazwa kamery, lokalizacja kamery, sygnatura czasowa, datownik „na żywo”, wskaźnik nagrywania, aktywność ruchu (miejsce występowania ruchu), zdarzenia analizy obrazu, tablice rejestracyjne, jakość wyświetlania obrazu w aplikacji klienckiej (co najmniej 3 różne poziomy) oraz regulacja ustawień wyświetlania obrazu (korekcja gamma, poziom czerni, poziom bieli).

Wyświetlanie obrazów w panelu głównym

- Panel główny musi umożliwiać oglądanie pełnych jakościowo obrazów, wsparcie dla kompresji co najmniej: MJPEG, JPEG2000, MPEG4, H.264;
- Panel główny musi umożliwiać tworzenie zakładek wraz panelami wideo do oglądu obrazów z kamer w trybie „na żywo” jak i nagranych materiałów wideo;
- Oprogramowanie musi mieć możliwość wykonywania zbliżeń z danej kamery z jednoczesną bezstratną rejestracją obrazu z całego pola widzenia kamery i optymalizacją wykorzystania pasma transmisji podczas tej operacji;
- W ramach jednej zakładki wideo system musi umożliwiać jednoczesne wyświetlanie do 64 obrazów (paneli wideo) łącznie z kamerami w podziale 8x8;
- Oprogramowanie musi zapewniać możliwość jednoczesnego wyświetlania na tym samym monitorze podłączonym do tej samej stacji klienckiej obrazu z wybranej kamery w trybie „na żywo” i „nagranych”;
- Aplikacja musi umożliwiać pracę na stanowisku wielomonitorowym – do co najmniej 6 monitorów łącznie;
- W ramach pracy wielomonitorowej aplikacja kliencka musi posiadać możliwość wyświetlania jej na każdym monitorze niezależnie w ramach nowo otwartych okien;
- Każde nowo otwarte okno musi tworzyć nowy panel główny z wszystkimi funkcjonalnościami opisanymi jako wymagania panelu głównego;
- W ramach wyświetlanych obrazów z kamer system musi umożliwiać wykonanie zdjęcia w zadanej przez operatora jakości i rozdzielczości wraz z opcją wyboru formatu i obszaru eksportu z danego kadru;
- W ramach zapisu zdjęcia system musi umożliwiać korektę ustawień gammy, poziomu czerni i bieli;
- Okno panelu wideo musi umożliwiać maksymalizację oglądu z danego źródła wideo jak i powrót do poprzedniej wielkości (przed wywołaniem trybu pełnoekranowego);
- W ramach panelu wideo system musi umożliwiać uruchamianie zapisu wideo w trybie manualnym;
- W ramach panelu wideo użytkownik musi mieć możliwość zamknięcia danego widoku z kamery (panelu wideo);
- System musi umożliwiać zapis danego widoku (układu paneli wideo wraz z obrazami i innymi danymi) wykorzystywanego przez użytkownika w celu późniejszego ponownego wykorzystania;
- W sytuacji wyświetlania obrazu z kamery PTZ system będzie umożliwiał jej sterowanie w zakresie

obrotu w pionie i poziomie, zoomu optycznego oraz cyfrowego;

- System musi umożliwiać w danym panelu wideo natychmiastowy dostęp na żądanie do materiału nagranych z ostatnich 30, 60 i 90 sekund;
- System musi posiadać funkcję cyfrowego zoomu w podglądzie na żywo oraz przy odtwarzaniu nagrań z archiwum;
- Oprogramowanie musi umożliwiać oglądanie tego samego strumienia wideo na żywo lub nagranych na różnych poziomach zoomu cyfrowego i na różnych obszarach widoku;
- Oprogramowanie musi umożliwiać nawigację na nagraniach wideo i audio poprzez kalendarz, linię czasu lub zdarzenia;
- System musi umożliwiać transmisję dźwięku w danym panelu wideo: od wideo serwera do oprogramowania klienckiego, obsługa dźwięku w podglądzie na żywo oraz w podglądzie przy odtwarzaniu nagrań z archiwum;
- System musi umożliwiać podgląd miniatury obrazów na liście (drzewie) kamer bez konieczności wyświetlania ich w panelu głównym.

Ustawianie parametrów pracy kamer

Oprogramowanie klienckie musi posiadać poniższe funkcjonalności związane z konfiguracją i parametryzacją pracy kamer. Wszystkie funkcjonalności muszą być dostępne z poziomu uprawnień administratora, jak również z poziomu uprawnień operatora o ile ma uprawnienia do zmiany części z nich.

- Oprogramowanie musi umożliwiać zmianę podstawowych parametrów kamery takich jak: nazwa kamery, lokalizacja kamery, logiczne ID;
- Oprogramowanie musi posiadać możliwość resetu (ponownego uruchomienia) kamery;
- Oprogramowanie musi posiadać możliwość nadawania kamerze adresu IP;
- Oprogramowanie musi umożliwiać włączenie multimedialnej transmisji (multicast) wraz z możliwością ustawienia TTL;
- Oprogramowanie musi umożliwiać wybór:
 - o typu kompresji obrazu kamery w ramach typów wykorzystywanych przez kamerę;
 - o ilości generowanych klatek na sekundę;
 - o jakości obrazu (stopnia kompresji);
 - o maksymalnej przepływności (bit rate);
 - o rozdzielczości pracy;
 - o odstęp pomiędzy klatkami kluczowymi;
- Oprogramowanie w ramach ustawienia parametryzacji pracy musi pokazywać daną chwilową przepływność (bit rate) przy danych parametrach pracy kamery;
- Oprogramowanie musi umożliwiać parametryzację nagrywania ręcznego (wyzwalanego przez operatora) z poziomu panelu wideo. Oprogramowanie musi umożliwiać ustawienie czasu nagrywania przed włączeniem i długości manualnego nagrywania w sytuacji włączenia go i nie wyłączenia przez operatora;
- Oprogramowanie musi umożliwiać konfigurację analizy wideo w kamerach pod warunkiem wykorzystania odpowiednich modeli kamer lub dedykowanych urządzeń zintegrowanych z VMS (szczegółowe wymagania w innej części dokumentu);
- Oprogramowanie musi umożliwiać konfigurację wejść i wyjść cyfrowych kamery (o ile kamera je posiada) oraz skutków wystąpienia danego zdarzenia dla pracy systemu nagrywania;
- Oprogramowanie musi posiadać możliwość elastycznego konfigurowania harmonogramu rejestracji obrazu z danej kamery przy użyciu kalendarza pozwalającego na wybór trybów pracy: rejestracja całości materiału, ruchu, zdarzeń, brak rejestracji przy jednoczesnym podglądzie „na żywo”, itp.;
- Oprogramowanie musi posiadać możliwość skalowania rozmiarów obrazu w sytuacji wykorzystania kamer z kompresją JPEG2000;

Sterowanie kamerami PTZ

Oprogramowanie musi posiadać poniższe funkcjonalności, których poprawna praca będzie zależała od poziomu integracji danej kamery z oprogramowaniem:

- Oprogramowanie serwerowe i klienckie musi umożliwiać zdalne sterowanie kamerami obrotowymi (Pan/Tilt/Zoom) różnych producentów;
- Oprogramowanie musi umożliwiać konfigurację co najmniej 10 programowalnych pozycji dla każdej kamery obrotowej;
- Oprogramowanie musi posiadać możliwość konfigurowania tras patrolowych w kamerze obrotowej (pod warunkiem zastosowania kamery odpowiedniego typu);
- Oprogramowanie musi posiadać możliwość wysterowania kamery obrotowej we wcześniej zaprogramowaną pozycję presetu poprzez zdarzenie alarmowe (detekcja ruchu, alarm, itp.);
- Oprogramowanie musi umożliwiać sterowanie kamerami obrotowymi przez uprawnione osoby na każdym stanowisku operatorskim w systemie za pomocą pulpitu sterującego zintegrowanego z komputerem PC i/lub konsoli wirtualnej wbudowanej w aplikację kliencką;

Wymagania dla oprogramowania w zakresie współpracy i obsługi analizy wideo (pod warunkiem wykorzystania odpowiednich modeli kamer lub dedykowanych urządzeń zintegrowanych z VMS)

- Oprogramowanie musi posiadać możliwość obsługi kamer wideo z wbudowaną analizą wideo;
- Oprogramowanie musi umożliwiać wyświetlanie alarmów generowanych przez daną analizę wideo wraz z zaznaczeniem na klatce miejsca zdarzenia;
- Oprogramowanie musi umożliwiać korelowanie alarmów generowanych przez analizę wideo z innymi scenariuszami obsługiwanymi przez aplikację kliencką;
- Oprogramowanie musi umożliwiać współpracę z zewnętrznymi urządzeniami analizy wideo wraz z przesyłaniem informacji z urządzenia do serwera i aplikacji klienckiej;
- Oprogramowanie musi umożliwiać w ramach istniejącego, wbudowanego interfejsu konfigurację analiz wideo, ich pracy, oraz typów alarmów przez nie wyzwalanych.

Szczegółowe wymagania dotyczące analizy wideo (pod warunkiem wykorzystania odpowiednich modeli kamer lub dedykowanych urządzeń zintegrowanych z VMS)

- Analiza wideo musi być oparta o tzw. „pattern analysis” – analiza oparta o wzorce;
- Analiza wideo musi umożliwiać analizę w oparciu o strumienie wysokiej rozdzielczości: od jakości SD (kamery analogowe) do 2Mpix włącznie;
- Operator musi mieć możliwość dodatkowej ingerencji w pracę algorytmów wideo – dodatkowa nauka analizy w oparciu o klasyfikację obiektów przez operatora;
- Analiza wideo musi posiadać wbudowane narzędzia do optymalizacji swojej pracy, uczenia się pracy w oparciu o otoczenie i jego charakterystykę;
- Analiza wideo musi umożliwiać detekcję i rozróżnianie obiektów – człowiek, pojazd;
- Operator musi posiadać możliwość tworzenia stref detekcji (pracy analizy wideo) oraz stref wyłączonych z analizy;
- Analiza wideo musi umożliwiać detekcję i alarmowanie w oparciu o co najmniej niniejsze reguły:
 - o wykrycie pojawienia się obiektu w obszarze zainteresowania;
 - o wykrycie wejścia jednego lub więcej obiektów w obszar zainteresowania z możliwością definiowania ilości obiektów wywołujących alarm;
 - o wykrycie przebywania obiektu w obszarze zainteresowania ponad zdefiniowany czas;
 - o wykrycie zatrzymania się (braku ruchu) obiektu w obszarze zainteresowania ponad zdefiniowany czas;
 - o wykrycie przekroczenia wirtualnej linii przez jeden lub więcej obiektów z możliwością definiowania ilości obiektów wywołujących alarm i kierunku przekroczenia linii;
 - o wykrycie zniknięcia obiektu z obszaru zainteresowania;
 - o wykrycie opuszczenia obszaru zainteresowania przez jeden lub więcej obiektów z możliwością definiowania ilości obiektów wywołujących alarm;
 - o wykrycie poruszania się obiektu w niedozwolonym kierunku;
 - o wykrycie nagłej zmiany sceny obserwowanej przez kamerę (spowodowanej np. sabotażem kamery).

Wymagania w zakresie administracji systemem

- Oprogramowanie musi prowadzić log zdarzeń obejmujący następujące zdarzenia dotyczące użytkowników: logowanie, wylogowania użytkownika, serwer zmienił ustawienie, ustawienia strony

zmienione, zmieniono ustawienie urządzenia, urządzenie podłączone, urządzenie odłączone, wyjście cyfrowe wyzwalone, dodanie zakładki, zakładka zaktualizowana, skasowanie zakładki, PTZ zmieniony, PTZ bezczynny, wykonanie eksport materiału o, aktywacja głośnika, głośnik wyłączony, otwarciu macierzy wirtualnej monitorów, mapa dodana, mapa aktualizowana, skasowanie mapy, widok dodany, widok zaktualizowany, widok usunięty, dodanie strony web, strona web zaktualizowana, strona web skasowana;

- Oprogramowanie musi zapisywać alarmy oraz informacje o systemie w bazie danych;
- Oprogramowanie musi prowadzić log zdarzeń obejmujący następujące zdarzenia na serwerze: uruchamianie serwera aplikacji, zamykanie serwera aplikacji, nieoczekiwana przerwa w działaniu serwera aplikacji, niski stan zasobów serwera aplikacji, błąd instalacji serwera aplikacji, licencja wkrótce wygaśnie, licencja wygasła, błąd bazy danych, błąd inicjalizacji danych, błąd partycji, powrót działania partycji, zmniejszony rozmiar do zapisu danych, błąd zapisu danych, rozpoczęcie uaktualnienia danych, aktualizacja danych zakończona, aktualizacja danych nie powiodła się, rozpoczęcie odzyskiwania danych, odzyskiwanie danych zakończone, odzyskiwanie danych nie powiodło się, zapisywanie zakładki nie powiodło się, połączenie sieciowe nawiązanie, połączenie sieciowe stracone, błąd wysyłania e-maila, błąd sprzętowy serwera, wykonywanie kopii zapasowej rozpoczęto, archiwizacja zakończona, kopia zapasowa nie powiodła się, połączenie z serwerem utracone;
- System musi zapewniać możliwość zdalnego przydzielania uprawnień dostępu przez administratorów systemu do różnych lokalizacji i serwerów z jednego miejsca;
- System musi umożliwiać autoryzację z wykorzystaniem skonfigurowanych i opisanych użytkowników wraz z możliwością importu użytkowników z domeny systemu Windows (Active Directory);
- System musi posiadać możliwość niezależnego przyporządkowania uprawnień każdemu z użytkowników systemu do co najmniej: podglądu na żywo, sterowania PTZ, blokowania sterowania PTZ, odtwarzania zarejestrowanego materiału, eksportu materiału wideo, konfiguracji systemu, zarządzania użytkownikami
- System musi posiadać funkcję raportowania o aktywności użytkownika oraz o zdarzeniach w systemie z możliwością zapisania wyników raportu do pliku;
- System musi umożliwiać centralne zarządzanie uprawnieniami wszystkich użytkowników systemu;
- Oprogramowanie musi posiadać możliwość monitorowania dostępu użytkownika do każdego klastra serwerów;
- Oprogramowanie musi zapewnić możliwość importowania i eksportowania ustawień, takich jak mapy, widoki i strony web;
- Oprogramowanie musi umożliwiać administrację systemu z dowolnej stacji operatorskiej włączonej do sieci komputerowej systemu monitoringu.

Mapy w systemie

- Oprogramowanie musi posiadać możliwość wykorzystania wielopoziomowych, hierarchicznych, przejrzystych map umożliwiających wskazanie zasięgu danej kamery na obiekcie;
- Mapy w systemie muszą być oparte co najmniej o pliki w formatach: jpeg, jpg, bmp, png, tiff;
- Oprogramowanie musi posiadać możliwość umieszczania na mapach punktów kamerowych wraz z graficznym określeniem zasięgu pola ich widzenia;
- Oprogramowanie musi posiadać możliwość wyboru kamery z poziomu mapy terenu;
- Oprogramowanie musi zapewniać możliwość natychmiastowego uzyskania obrazu z wybranej kamery poprzez kliknięcie „ikony kamery” na mapie wraz z uzyskaniem predefiniowanych obrazów z danej kamery np. sceneria ogólna wraz z jednoczesną wizualizacją wybranych miejsc w polu widzenia danej kamery (wybór z poziomu listy, mapy terenu);
- Oprogramowanie musi umożliwiać wyświetlenie miniatury obrazu z kamery po wskazaniu jej ikony kursorem na mapie
- Mapy muszą być aktywne tzn. pokazywać zdarzenia alarmowe w sytuacji wyzwolenia alarmu przez daną kamerę;
- Mapy muszą umożliwiać nanoszenie ikon kamer w różnych kolorach.

Eksport materiału wideo

- W ramach eksportu materiału w formacie macierzystym oprogramowanie musi umożliwiać jednoczesny eksport z jednej lub wielu kamer jednocześnie – w ramach jednego pliku do odtwarzania, z różnych przedziałów czasowych dla jednej lub wielu kamer;
- Oprogramowanie musi umożliwiać określenie długości eksportowanego materiału wideo w oparciu o kalendarz jak i zaznaczenie zakresu na osi czasu;
- W ramach eksportu materiału musi istnieć możliwość wyboru maksymalnego rozmiaru generowanych plików w zakresie: brak ograniczeń i powszechnie stosowane wielkości płyt np. CD, DVD, Blu-Ray;
- Oprogramowanie musi umożliwiać konwersję materiału wideo, który został wyeksportowany w natywnym formacie do innych popularnych formatów takich jak PNG, JPEG, TIFF, PDF;
- W ramach eksportu do innego formatu niż macierzysty musi istnieć możliwość zmiany rozdzielczości eksportowanego pliku oraz regionu eksportu (wybranego fragmentu z całego kadru);
- Oprogramowanie musi posiadać funkcję dołączania do eksportowanych nagrań programu do ich odtwarzania;
- Oprogramowanie musi zapewniać możliwość eksportu materiału wideo z wielu określonych (zdarzeń) przedziałów czasowych jednocześnie;
- Oprogramowanie musi zapewniać możliwość eksportu materiału z kamer typu fisheye w ich naturalnej „wyprostowanej/de-warped” postaci.

Wyszukiwanie zdarzeń

- Oprogramowanie musi umożliwiać przeszukiwanie zarejestrowanego obrazu i dźwięku w oparciu o różne kryteria, w tym o czas, datę, źródła wideo i zdarzenia;
- Oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo na podstawie ruchu w obszarach zdefiniowanych przez użytkownika;
- Oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo w oparciu o czas, datę, źródła wideo i wyświetlić wyniki jako serię miniatur;
- Oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo w oparciu o zdarzenia alarmowe;
- Oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo w oparciu o transakcje z urządzeń transakcji tekstowych, np. POS;
- Oprogramowanie musi zapewniać możliwość i wsparcie programowe wyszukiwania zdarzeń w aplikacji klienckiej (dla kamer wyposażonych w odpowiednią analizę obrazu) w oparciu o kategoryzację obiektów jak człowiek i samochód.

Alarmowanie i obsługa alarmów

- System musi mieć możliwość generowania i eskalowania alarmów w oparciu o czas wystąpienia i priorytet;
- Oprogramowanie musi umożliwiać obserwację stanu wejść alarmowych, ciągle monitorowanie i powiadomianie (z wyświetlaniem odpowiedniego komunikatu) o każdym zaniku sygnału, zasilania, otwarciu drzwi, itp.;
- Oprogramowanie musi rejestrować zdarzenia alarmowe w bazie zawierającej datę, czas wystąpienia i opis zdarzenia;
- Oprogramowanie musi posiadać możliwość elastycznego kreowania reguł definiujących automatyczne reakcje systemu na dane zdarzenia (system umożliwia automatyczne reagowanie na wcześniej zdefiniowane zdarzenia i alarmy);
- Oprogramowanie musi posiadać możliwość stworzenia alarmów dedykowanych dla głównej stacji monitorowania (o najwyższym priorytecie);
- Oprogramowanie musi posiadać możliwość wysyłania informacji o zdarzeniach poprzez e-mail;
- Oprogramowanie musi posiadać możliwość przyjmowania alarmów i zdarzeń z systemów trzecich poprzez ONVIF wraz z możliwością ich wyszukiwania w aplikacji zarządzającej.

Oprogramowanie musi reagować na co najmniej poniższe typy zdarzeń wyzwalając odpowiednie reguły systemu:

- Zdarzenia serwera
 - o Uruchomienie aplikacji serwera;
 - o Zamykanie aplikacji serwera;

- o Aplikacja serwera nieoczekiwanie zakończyła pracę;
- o Małe zasoby aplikacji serwera;
- o Błąd instalacji aplikacji serwera;
- o Licencja wkrótce wygasa;
- o Licencja wygasła;
- o Błąd bazy danych;
- o Błąd inicjowania danych;
- o Błąd wolumenu danych;
- o Odzyskano wolumen danych;
- o Zmniejszono wolumen danych;
- o Błąd zapisu danych;
- o Rozpoczęto uaktualnianie danych;
- o Zakończono uaktualnianie danych;
- o Uaktualnianie danych zakończone niepowodzeniem;
- o Rozpoczęto odzyskiwanie danych;
- o Zakończono odzyskiwanie danych;
- o Odzyskiwanie danych zakończone niepowodzeniem;
- o Zapisywanie zakładki zakończone niepowodzeniem;
- o Znaleziono połączenie sieciowe;
- o Utrata połączenia sieciowego;
- o Błąd wysyłania e-mail;
- o Archiwizowanie rozpoczęte;
- o Archiwizowanie zakończone;
- o Archiwizowanie zakończone niepowodzeniem;
- o Utrata połączenia z serwerem;
- Zdarzenia urządzenia
 - o Połączenie utworzone;
 - o Połączenie usunięte;
 - o Utworzono połączenie z serwerem rezerwowym;
 - o Połączenie z serwerem rezerwowym usunięte;
 - o Błąd połączenia;
 - o Połączenie przywrócone;
 - o Niedopuszczalna utrata pakietu sieciowego;
 - o Dopuszczalna utrata pakietu sieciowego;
 - o Rozpoczęto wykrywanie ruchu;
 - o Zakończono wykrywanie ruchu;
 - o Zostało rozpoczęte zdarzenie analizy obrazu wideo;
 - o Zdarzenie analizy obrazu wideo zostało zakończone;
 - o Wykryto ingerencję;
 - o Nagrywanie rozpoczęte, zakończone, przerwane, wznowione;
 - o Wejście cyfrowe aktywowane, dezaktywowane.
- Zdarzenia użytkownika
 - o Logowanie i wylogowanie użytkownika;
 - o Ustawienia serwera zmienione;
 - o Ustawienia witryny zmienione;
 - o Ustawienia urządzenia zmienione;
 - o Urządzenie podłączone, odłączone;
 - o Wyjście cyfrowe wyzwolone;
 - o Zakładka dodana;
 - o Zakładka zaktualizowana;
 - o Zakładka usunięta;
 - o PTZ przeniesiony;
 - o PTZ bezczynny;
 - o Przeprowadzono eksport;

- o Głośnik aktywowany, dezaktywowany;
- o Monitor wirtualny otwarty;
- o Mapa dodana;
- o Mapa zaktualizowana;
- o Mapa usunięta;
- o Widok dodany.
- Zdarzenia alarmu
 - o Alarm zatwierdzony;
 - o Alarm automatycznie zatwierdzony;
 - o Włączony alarm;
 - o Alarm przypisany;
 - o Usunięto przypisanie alarmu;
 - o Alarm wyczyszczony.
- Zdarzenia transakcji POS (jeśli ten moduł jest aktywny w systemie)
 - o Transakcja POS rozpoczęta;
 - o Transakcja POS zakończona;
 - o Wyjątek transakcji POS.
- Zdarzenia LPR/ANPR (jeśli ten moduł jest aktywny w systemie)
 - o Rozpoczęto wykrywanie tablicy rejestracyjnej;
 - o Zakończono wykrywanie tablicy rejestracyjnej;
 - o Zgodność z listą numerów rejestracyjnych

5. Minimalne wymagania dla urządzenia rejestrującego

Komponent	Parametry nie gorsze niż:
Płyta główna	Jednoprocesorowa, serwerowa posiadająca: <ul style="list-style-type: none"> • możliwość instalacji modułu TPM • min. jedno złącze PCI-E x 16 (mechanicznie i elektrycznie) • min. 3 złącza PCI-E x 8 (mechanicznie i elektrycznie) • obsługująca procesory serii Xeon® Scalable Processors • min. 3 złącza USB 3.0, tym jedno typu A wewnątrz serwera • min. 8 złączy DIMM • zintegrowany kontroler IPMI 2.0 z dedykowanym złączem RJ45
Procesor	Zainstalowany co najmniej jeden procesor o co najmniej 8 rdzeniach, taktowany zegarem min. 2,1GHz, wyposażony w co najmniej 12 MB pamięci cache, umożliwiający osiągnięcie w teście Passmark – CPU Mark wyniku min. 18000 pkt. (wynik na dzień 01.02.2022).
Karty graficzne	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości min. 1280x1024 pikseli, współpracująca z kartą zarządzającą.
Karty sieciowe	Min. 2 porty Ethernet 10GBase-T wbudowane na płycie głównej i nie zajmujące gniazd PCI-E. Dodatkowa karta z min. 2 portami 1Gbps RJ-45.
Zarządzanie	Niezależna od zainstalowanego systemu operacyjnego dedykowana karta zarządzająca z dostępem przez dedykowany port RJ-45 Gigabit Ethernet umożliwiająca: <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu web karty zarządzającej • zdalne monitorowanie i informowanie o statusie serwera (temperaturze, prędkości obrotowej wentylatorów itd.) • szyfrowane połączenie w sieci (SSL v3 lub TLS) • włączenie, wyłączenie i restart serwera • podgląd logów sprzętowych serwera i karty • przejście pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS) • możliwość montowania zdalnych wirtualnych napędów, plików ISO

Pamięć RAM	Min. 32GB DDR4 ECC o częstotliwości min. 2667MT/s możliwość rozbudowy do min. 256GB.
Kontroler RAID	Sprzętowy, kontroler RAID SAS 12Gb/s i SATA 6Gb/s posiadający następujące funkcjonalności: <ul style="list-style-type: none"> • obsługa poziomów RAID 0, 1, 10, 5, 50, 6, 60 • posiadający min. 1GB pamięci cache • posiadający moduł zabezpieczenia pamięci cache przed utratą zasilania • obsługa min. 60 dysków
Dyski	Przeźreń dyskowa musi umożliwić ciągle (24/7) zapis wideo ze wszystkich kamer przez okres 30 dni, przy założeniu 13 kl/s z każdej kamery. Przeźreń ta musi być zapewniona przez zastosowanie serwerowych dysków twardych SAS/SATA o MTBF min. 2 miliony godzin i 5 letniej gwarancji producenta skonfigurowanych jako jedna lub więcej macierzy RAID 5 z dodatkowym dyskiem hot spare. Liczba dysków w ramach jednej macierzy RAID nie może przekroczyć 12. Efektywna pojemność pojedynczego wolumenu widzianego przez system operacyjny nie może przekroczyć 50 TB. Zainstalowane dyski muszą być kompatybilne z oferowanym kontrolerem RAID (według listy kompatybilności producenta kontrolera RAID lub producenta dysków). Dwa dyski SSD przeznaczone na system operacyjny i przystosowane do pracy w serwerach, każdy o pojemności min. 240GB i MTBF min. 2 miliony godzin pracujące w konfiguracji RAID 1.
Obudowa	Typu rack 19" o wysokości 2U wraz z zestawem montażowym umożliwiającym montaż w typowej, 19-calowej szafie serwerowej, w tym pełne wysunięcie serwera z szafy, posiadająca: <ul style="list-style-type: none"> • Dwa zasilacze hot swap o mocy co najmniej 600W każdy i sprawności min. 94% przy obciążeniu 50%. • Zasilacze muszą posiadać certyfikat Platinum Level Certified. Wymagane dołączenie raportu do oferty. • Obudowa musi umożliwiać instalację min. 12 dysków SAS 12Gb/s / SATA / SSD w formacie 3.5" oraz dodatkowo posiadać 2 kieszenie na dyski 2.5" (wolne zatoki na dyski obsadzone ramkami hot-swap, możliwość dodania własnego dysku przez użytkownika bez konieczności zakupu specjalnej ramki). • Zasilacze, dyski, wentylatory muszą być elementami typu „hot swap”. • Obudowa musi posiadać przednią osłonę na dyski twarde zamykaną na klucz • Obudowa musi zawierać wszystkie niezbędne elementy do rozbudowy serwera o dodatkowe półki dyskowe.
System operacyjny	Microsoft Windows Server Standard 2019 16 core lub Windows Server IoT 2019 for Storage Standard (16 core) lub odpowiedni nowszy
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-1401 • Oznaczenie CE • Oferowany model serwera musi znajdować się na liście Windows Server Catalog i posiadać status Certified for Windows dla systemów Windows Server 2019/2022. Wymagany wydruk ze strony https://www.windowsservercatalog.com
Gwarancja	Gwarancja minimum 36 miesięcy w trybie serwisu w miejscu instalacji serwera (on-site), czas reakcji 4h, czas naprawy w następnym dniu roboczym. Możliwość telefonicznego zgłaszania usterek w serwisie producenta. Wymagany okres przyjmowania zgłoszeń serwisowych we wszystkie dni robocze. W przypadku uszkodzenia dysku twardego (HDD) uszkodzony dysk pozostaje u Zamawiającego.
Wsparcie techniczne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Inne	<p>Dostarczony sprzęt musi być fabrycznie nowy. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne.</p> <ul style="list-style-type: none"> • Serwer musi być kompatybilny z systemem VMS • Serwer musi mieć preinstalowaną aplikację serwerową systemu VMS • Do serwera należy dostarczyć licencje oprogramowania VMS do obsługi wymaganej liczby kanałów wideo • Serwer musi posiadać zainstalowany moduł umożliwiający wizualizację warunków jego pracy (temperatura CPU, prędkości wentylatorów, stan otwarcia obudowy) w systemie VMS
------	---

6. Minimalne wymagania dla stacji roboczych

Wyświetlanie strumieni wideo	do 144 strumieni wideo z kamer 2MP/25fps jednocześnie
Procesor	Intel® Core™ i9-11900KF lub wydajniejszy
Pamięć RAM	min. 32GB DDR4 3200MHz
Dysk	SSD NVMe M.2 o pojemności min. 500GB
Karta graficzna	Nvidia PNY Quadro P1000-V2 4GB GDDR5 lub wydajniejsza
Interfejs sieciowy	2 x Gigabit Ethernet RJ-45 (1000Base-T)
Obudowa	typu mini-tower lub desktop
Akcesoria	klawiatura USB, mysz USB
System operacyjny	Microsoft Windows 10 Professional lub nowszy
Gwarancja	Gwarancja minimum 36 miesięcy w trybie serwisu w miejscu instalacji stacji (on-site), czas reakcji 4h, czas naprawy w następnym dniu roboczym. Możliwość telefonicznego zgłaszania usterek w serwisie producenta. Wymagany okres przyjmowania zgłoszeń serwisowych we wszystkie dni robocze.
Inne	Dostarczony sprzęt musi być fabrycznie nowy. Stacja musi być kompatybilna z systemem VMS i być wyposażona w preinstalowaną aplikację kliencką systemu VMS.

7. Minimalne wymagania dla okablowania strukturalnego

7.1 okablowanie zewnętrzne

- Kategoria ANSI/TIA – 7
- Typ komponentu kabla – Poziomy
- Rodzaj kabla - S/FTP (ekranowany)
- Typ przewodnika, pojedyncze – Drut
- Przewodniki, ilość – 8
- Kolor osłony – Czarny
- Pary, ilość – 4
- Standardy transmisji - ANSI/TIA-568.2D, CENELEC EN 50288-4-1, ISO/IEC 11801 klasa F
- Długość kabla - 500 m | 1640,42 FT
- Średnica na płaszczu, nominalna - 9,652 mm | 0,38 cala
- Grubość przewodu, pojedynczy - 23 AWG
- Charakterystyczna impedancja - 100 omów

- Charakterystyczna impedancja Tolerancja - ± 15 omów
- Pojemność wzajemna przy częstotliwości - 4,1 nF/100 m przy 1 kHz
- Nominalna prędkość propagacji (NVP) - 82 %
- Napięcie robocze, maksymalne - 80 V
- Napięcie znamionowe - 240 V
- Materiał przewodnika - Czysta miedź
- Materiał izolacyjny – Poliolefina
- Materiał osłony – PE
- Materiał osłony wewnętrznej - Bezhalogenowy o niskiej emisji dymu (LSZH)
- Temperatura instalacji - 0 °C do +50 °C (+32 °F do +122 °F)
- Temperatura pracy - - 20 °C do +60 °C (-4 °F do +140 °F)
- EN50575 Kabel CPR Euroklasa Odporność ogniowa – Fca
- Przestrzeń środowiskowa - Odporny na promieniowanie UV na zewnątrz i Low Smoke Zero Halogen
- CENELEC - Zgodny z normą EN 50575, dostępna deklaracja właściwości użytkowych
- CHINY-ROHS - (DoP) Poniżej maksymalnej wartości stężenia
- REACH-SVHC - Zgodny zgodnie z wersją SVHC
- ROHS - Zgodny

7.2 okablowanie wewnętrzne

- Czteroparowy kabel symetryczny 1427213 o konstrukcji F/UTP i szerokości pasma przenoszenia 250 MHz charakteryzuje się doskonałymi parametrami transmisyjnymi oraz ekranowaniem, co sprawia, że nadaje się on do stosowania w systemach okablowania klasy E jako produkt kategorii 6.
- Przeznaczony jest do zastosowań w sieciach LAN oraz w sieciach szerokopasmowych. Kabel w pełni zgodny z zaleceniami normy IEEE 802.3bt (typ 4) 4Pary PoE (Power over Ethernet), dotyczącymi bezpiecznego dostarczania zasilania przez kabel LAN PoE gdy jest zainstalowany zgodnie z ISO / IEC 14763-2, CENELEC EN 50174-1, CENELEC EN 50174-2 lub TIA TSB- 184-A konstrukcja F/UTP, naokoło czterech par folia aluminiowa, dodatkowo separator w środku oddzielający pary i poprawiający parametry transmisyjne
- wydajność transmisyjna określona do 250 MHz
- przewyższa wymagania dla produktu kategorii 6 zgodnie z ANSI/TIA-568-C.2, ISO/IEC 11801 Class E
- koszulka zewnętrzna z materiału LSZH (Low Smoke Zero Halogen)
- palność określona zgodnie z EN50575 CPR Dca
- kabel przetestowany na brak wydzielanie dymu podczas palenia zgodnie z IEC 61034-2
- kabel przetestowany na brak propagacji płomienia podczas palenia zgodnie z INEC Article 800 | UL 444
- temperatura pracy: -20° do +60° C
- temperatura instalacji: 0° do +60° C
- średnica przewodnika - AWG23 (0.55 mm)
- ilość par – 4
- średnica zewnętrzna - 7.188 mm
- pasmo przenoszenia - 250 MHz

UWAGA: Wszystkie systemy odpowiadające za bezpieczeństwo obiektu Zapora w Pieczyskach, muszą pochodzić z legalnego, autoryzowanego kanału dystrybucji w Polsce oraz posiadać autoryzowane wsparcie producenta wraz serwisem realizowanym na terenie państwa Polskiego.