Specyfikacja systemu monitoringu

Minimalne wymagania techniczne do kamer

Kamera typ 1, kamery do obserwacji trybun.

Kamera zewnętrzna typu turet 16,5Mpx
• Przetwornik CMOS nie mniejszy niż 1/1.8”
• Kamera musi zapewniać możliwość generowania pojedynczego strumienia rozdzielczości min. 16,5 Megapiksela
• Kamera musi zapewnić możliwość obsługi min. dwóch niezależnych sensorów optycznych
• Ilość efektywnych pikseli pojedynczego przetwornika nie mniejsza niż 8,42 Megapikseli
• Powierzchnia piksela na przetworniku nie mniejsza niż 4,00 um2
• Światłoczułość przetwornika powinna wynosić przynajmniej 30,000e-/Lux·sec
• Kąt widzenia min. 95°x50°
• Możliwość przesyłania video z prędkością 30 ramek na sekundę w rozdzielczości 3840x2160 lub większej.
• Kamera musi być wyposażona w przetwornik z WDR o mocy przynajmniej 120 dB.
• Kamera musi obsługiwać kodowanie obrazu H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265 oraz nie dopuszcza się stosowania licencji MPGLA dla H.265
• Kamera musi zapewnić obsługę następujących kodeków MJPEG/H.264/H.265
• Kamera musi być wyposażona w promiennik podczerwieni odseparowany fizycznie od obiektywu, celem uniknięcia oślepiania. Przemiennik powinien pracować w zakresie 850-860nm.
• Kamera musi umożliwiać łatwą wymianę promiennika podczerwieni w celu dopasowania odpowiedniego zasięgu i kąta widzenia. Promiennik podczerwieni powinien być sterowany przez kamerę wykorzystując sygnał na wejściu alarmowym, zewnętrzną komendę HTTP, poprzez harmonogram, oraz poprzez zakres ilości LUX na samym przetworniku
• Procesor kamery musi umożliwiać wykrycie oraz klasyfikację obiektu (człowiek, pojazd, zwierzę)
• W przypadku wystąpienia alarmu na kamerze (analiza obrazu, zanik sieci, sabotaż kamery, zdarzenie cykliczne, naruszenie wejścia alarmowego w kamerze), kamera musi posiadać możliwość wysłania komendy CGI na wybrany adres sieciowy
• Kamera musi posiadać przynajmniej 1 wejście alarmowe oraz 1 wyjście. Dopuszcza się stosowanie zewnętrznych modułów rozszerzających, jeśli będą dostarczone, zamontowane i skonfigurowane razem z kamerami,
• Kamera musi posiadać certyfikację ONVIF zapewniająca kompatybilność z innymi urządzeniami
• Kamera musi wspierać następujące profile standardu ONVIF: S, T,
• Obudowa kamery musi posiadać szczelność minimalnie IP66, oraz odporność na uderzenia na poziomie IK10

• Kamera musi posiadać możliwość pracy przy szerokim zakresie temperatur, przynajmniej -40 do +60.
• Kamera musi posiadać interfejs sieciowy o przepustowości 1000Mbps
• Kamera musi posiadać port USB umożliwiający podłączenie zewnętrznych pamięci
• Kamera musi być wyposażona w kartę SD min. 8GB

Kamera typ 2: kamery obserwujące boisko główne

•Przetwornik CMOS nie mniejszy niż 1 /1.8”

• Sumaryczna ilość pikseli przetwornika nie mniejsza niż 9,17Mpx, a ilość efektywnych pikseli przetwornika nie mniejsza niż 8.42 Megapikseli

• Powierzchnia pojdynczego piksela na przetworniku nie mniejsza niż 4 um2

• Światłoczułość przetwornika powinna wynosić przynajmniej 30,000e-/Lux·sec

• Kamera wyposażona w obiektyw zapewniający kąty widzenia (horyzontalne) w zakresie >112˚ do <48˚ (najszerszy kąt może być większy. Dopuszcza się większy zakres – mniejszy kąt po przybliżeniu). Obiektyw musi posiadać funkcję zdalnego ustawiania ogniskowej i ostrości.

• Obiektyw o jasności przynajmniej F1.5 dla początku ogniskowej. Obiektyw musi posiadać sterowanie przysłoną wykorzystującą P-Iris, nie dopuszcza się kamer z DC-Iris

• Możliwość przesyłania video z prędkością 30 ramek na sekundę w rozdzielczości 3864x2180 lub większej.

• Obsługa przynajmniej 3 strumieniu obrazu, z czego przynajmniej dwa muszą obsługiwać rozdzielczość 3864x2180 i prędkości do 20 ramek na sekundę.

• Procesor obrazu musi posiadać wystarczającą moc obliczeniową do wygenerowania przynajmniej 3 strumieni w rozdzielczości FullHD, z czego jeden w 60 ramek na sekundę, a pozostałych w pełnych 30 ramkach na sekundę.

• Kamera musi być wyposażona w przetwornik Multi Exposure HDR o mocy przynajmniej 120 dB. Nie dopuszcza się samej technologii WDR.

• Kamera musi obsługiwać kodowanie obrazu H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265, nie dopuszcza się licencji MPGLA)

• Kamera musi posiadać możliwość wygenerowania strumienia FullHD w MJPEG z prędkością przynajmniej 30 ramek na sekundę

• Promiennik podczerwieni z minimalnym zasięgiem 40m, pracujący w zakresie 850nm lub 920nm

• Przetwornik kamery musi posiadać QE przynajmniej 60% dla zakresu podczerwieni wykorzystywanego w zamontowanych diodach "

Procesor kamery:

• Kamera musi posiadać procesor wyposażony w przynajmniej 4 rdzenie, taktowane 1Ghz.

• Procesor kamery musi umożliwiać obsłużenie następujących analityk obrazu bezpośrednio na kamerze:
o Detekcja porzuconego obiektu
o Rozpoznawanie twarzy z funkcją białej i czarnej listy na pokładzie kamery
o Rozpoznawanie tablic rejestracyjnych z funkcją białej i czarnej listy na pokładzie kamery
o Detekcja intruza w strefie
o Detekcja sabotażu obrazu kamery
o Niewłaściwy kierunek poruszania w strefie
o Detekcja podejrzanego wałęsania się
o Liczenie obiektów
o Detekcja usunięcia obiektu
o Detekcja zatrzymanego pojazdu"
Interfejsy i integracja
"• Kamera musi posiadać wejście i wyjście AUDIO. Rejestracja i przesyłanie dźwięku musi odbywać się z wykorzystaniem kodowania AAC lub MP3.
• W przypadku wystąpienia alarmu na kamerze (analiza obrazu, zanik sieci, sabotaż kamery, zdarzenie cykliczne, naruszenie wejścia alarmowego w kamerze), kamera musi posiadać możliwość wysłania komendy CGI na wybrany adres sieciowy
• Kamera musi posiadać przynajmniej 2 wejścia alarmowe oraz 1 wyjście. Dopuszcza się stosowanie zewnętrznych modułów rozszerzających, jeśli będą dostarczone, zamontowane i skonfigurowane razem z kamerami,
• Kamera musi posiadać certyfikację ONVIF zapewniająca kompatybilność z innymi urządzeniami
• Kamera musi wspierać następujące profile standardu ONVIF: S, G, T, Q
• Obudowa kamery musi posiadać szczelność minimalnie IP66, oraz odporność na uderzenia na poziomie IK10
• Kamera musi posiadać możliwość pracy przy szerokim zakresie temperatur, przynajmniej -50 do +60. Dopuszcza się stosowanie zewnętrznych grzałek, o ile będą automatycznie uruchamiane w przypadku spadku temperatury, oraz zasilane będą z tego samego źródła co kamera.
• Kamera musi umożliwiać zasilenie z różnych źródeł PoE + 12VDC lub 24AC. Zasilanie musi umożliwiać redundancje – w przypadku zaniku jednego ze źródeł, kamera powinna automatycznie bez restartu przełączyć się na zapasowe źródło. """
"• Przetwornik CMOS nie mniejszy niż 1 /2.8”
• Ilość efektywnych pikseli przetwornika nie mniejsza niż 3.2 Megapikseli
• Powierzchnia piksela na przetworniku nie mniejsza niż 6.25 um2
• Światłoczułość przetwornika powinna wynosić przynajmniej 10,000e-/Lux·sec
• Kamera wyposażona w moduł moto-zoom z 40x przybliżeniem, zapewniający kąty widzenia (horyzontalne) w zakresie >62˚ do <2˚ (najszerszy kąt może być większy. Dopuszcza się większy zakres – mniejszy kąt po przybliżeniu). Obiektyw musi posiadać funkcję zdalnego ustawiania ogniskowej i ostrości.
• Obiektyw o jasności przynajmniej F1.6 dla początku ogniskowej. Obiektyw musi posiadać możliwość sterowania przysłoną wykorzystując P-Iris lub Auto-Iris
• Możliwość przesyłania video z prędkością 30 ramek na sekundę w rozdzielczości 2065 x 1553 lub większej.
• Obsługa przynajmniej 3 strumieniu obrazu, z czego przynajmniej dwa muszą obsługiwać rozdzielczość 2Mpx i prędkości 30 ramek na sekundę.
• Kamera musi być wyposażona w przetwornik z WDR o mocy przynajmniej 120 dB
• Kamera musi obsługiwać kodowanie obrazu MJPEG, H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265)

• Promiennik podczerwieni z minimalnym zasięgiem 200m, pracujący w zakresie 850nm lub 920nm, z regulowaną mocą zależna od zbliżenia kamery
• Kamera musi posiadać elektroniczną stabilizację obrazu
• Silnik kamery PTZ musi posiadać możliwość rejestracji położenia w celu niwelacji przesunięcia względem presetów. Po siłowym przesunięciu modułu kamery, moduł musi wrócić do ostatniej pozycji zachowując współrzędnie presetów. Współrzędne modułu PTZ powinny być wyświetlane na OSD kamery.
• Kamera musi umożliwiać utworzenie minimalnie 8 sekwencji, 8 tras oraz 64 presetów.
• Moduł PTZ powinien umożliwiać prace z prędkością 0.1°/s do 300°/s
• Kamera musi posiadać wejście i wyjście AUDIO. Rejestracja i przesyłanie dźwięku musi odbywać się z wykorzystaniem kodowania AAC lub MP3.
• Kamera musi posiadać przynajmniej 4 wejścia alarmowe oraz 2 wyjścia alarmowe. Dopuszcza się stosowanie zewnętrznych modułów rozszerzających, jeśli będą dostarczone, zamontowane i skonfigurowane razem z kamerami,
• Kamera musi posiadać certyfikację ONVIF zapewniająca kompatybilność z innymi urządzeniami
• Kamera musi wspierać następujące profile standardu ONVIF: S, G, T
• Obudowa kamery musi posiadać szczelność minimalnie IP66, oraz odporność na uderzenia na poziomie IK10
• Kamera musi posiadać możliwość pracy przy szerokim zakresie temperatur, przynajmniej -50° do +55°.
• Kamera musi umożliwiać zasilenie z różnych źródeł UPoE lub HighPoE + 12VDC lub 24AC. Zasilanie musi umożliwiać redundancje – w przypadku zaniku jednego ze źródeł, kamera powinna automatycznie bez restartu przełączyć się na zapasowe źródło. "

Kamera typ 3, PTZ- obrotowa

• Przetwornik CMOS nie mniejszy niż 1 /2.8”
• Ilość efektywnych pikseli przetwornika nie mniejsza niż 3.2 Megapikseli
• Powierzchnia piksela na przetworniku nie mniejsza niż 6.25 um2
• Światłoczułość przetwornika powinna wynosić przynajmniej 10,000e-/Lux·sec
• Kamera wyposażona w moduł moto-zoom z 40x przybliżeniem, zapewniający kąty widzenia (horyzontalne) w zakresie >62˚ do <2˚ (najszerszy kąt może być większy. Dopuszcza się większy zakres – mniejszy kąt po przybliżeniu). Obiektyw musi posiadać funkcję zdalnego ustawiania ogniskowej i ostrości.
• Obiektyw o jasności przynajmniej F1.6 dla początku ogniskowej. Obiektyw musi posiadać możliwość sterowania przysłoną wykorzystując P-Iris lub Auto-Iris
• Możliwość przesyłania video z prędkością 30 ramek na sekundę w rozdzielczości 2065 x 1553 lub większej.
• Obsługa przynajmniej 3 strumieniu obrazu, z czego przynajmniej dwa muszą obsługiwać rozdzielczość 2Mpx i prędkości 30 ramek na sekundę.
• Kamera musi być wyposażona w przetwornik z WDR o mocy przynajmniej 120 dB
• Kamera musi obsługiwać kodowanie obrazu MJPEG, H.264 High Profile oraz H.265 (nie dopuszcza się kamer bez wymaganej licencji HEVC Advanced do używania kodeka H.265)
• Promiennik podczerwieni z minimalnym zasięgiem 200m, pracujący w zakresie 850nm lub 920nm, z regulowaną mocą zależna od zbliżenia kamery
• Kamera musi posiadać elektroniczną stabilizację obrazu
• Silnik kamery PTZ musi posiadać możliwość rejestracji położenia w celu niwelacji przesunięcia względem presetów. Po siłowym przesunięciu modułu kamery, moduł musi wrócić do ostatniej pozycji zachowując współrzędnie presetów. Współrzędne modułu PTZ powinny być wyświetlane na OSD kamery.

• Kamera musi umożliwiać utworzenie minimalnie 8 sekwencji, 8 tras oraz 64 presetów.
• Moduł PTZ powinien umożliwiać prace z prędkością 0.1°/s do 300°/s
• Kamera musi posiadać wejście i wyjście AUDIO. Rejestracja i przesyłanie dźwięku musi odbywać się z wykorzystaniem kodowania AAC lub MP3.
• Kamera musi posiadać przynajmniej 4 wejścia alarmowe oraz 2 wyjścia alarmowe. Dopuszcza się stosowanie zewnętrznych modułów rozszerzających, jeśli będą dostarczone, zamontowane i skonfigurowane razem z kamerami,
• Kamera musi posiadać certyfikację ONVIF zapewniająca kompatybilność z innymi urządzeniami
• Kamera musi wspierać następujące profile standardu ONVIF: S, G, T
• Obudowa kamery musi posiadać szczelność minimalnie IP66, oraz odporność na uderzenia na poziomie IK10
• Kamera musi posiadać możliwość pracy przy szerokim zakresie temperatur, przynajmniej -50° do +55°.
• Kamera musi umożliwiać zasilenie z różnych źródeł UPoE lub HighPoE + 12VDC lub 24AC. Zasilanie musi umożliwiać redundancje – w przypadku zaniku jednego ze źródeł, kamera powinna automatycznie bez restartu przełączyć się na zapasowe źródło.

Minimalne wymagania techniczne do rejestratora CCTV IP

Rejestrator do min 118 kamer

- CPU PASS MARK minimum: 19000 punktów
- Min procesory E-2324G - 3.1 GHz - 4C/4T
- Min 2 karty LAN 10Gb
- Min 16 zatok na dyski twarde Hot-Swap
- sprzętowy kontroler RAID 0, 1, 5, 6, 10, 50, 60, wyposażony w 8GB RAM
- 32B pamięci RAM 2666
- Zasilacz 1000W Platinum, skuteczność 80+, możliwość montażu dodatkowego redundantnego zasilacza
- Min 3 wentylatory 80mm hot-swap
- Możliwość instalacji systemu Linux lub Windows na dedykowanym dysku SSD (system z dyskiem dostarczony wraz z serwerem)
- Gwarancja 36 miesięcy On-Site NBD Advance Replacement
- Naprawa na miejscu instalacji urządzenia, czas przybycia serwisu 24h, naprawa do 3 dni roboczych.
- Zasilanie Redundantne

Minimalne wymagania techniczne do stacji klienckiej systemu CCTV IP

- CPU PASS MARK minimum: 8800 punktów
- Procesor do dekodowania H.264 i H.265, PASSMARK Min.: 1300 punktów
- Wyjście na monitor z obsługa rozdzielczości 4096 x 2304@60Hz 24bit
- Obsługa do 4 niezależnych wyświetlaczy
- 32 GB pamięci RAM 2666
- Obsługa min 4 dysków HDD + 4 dyski SSD
- Zasilacz 350W Platinium, skuteczność 80+
- Możliwość instalacji systemu Linux lub Windows na dedykowanym dysku (system dostarczony wraz z serwerem)
- Gwarancja 36 miesięcy On-Site NBD Advance Replacement

- Naprawa na miejscu instalacji urządzenia, czas przybycia serwisu 24h, naprawa do 3 dni roboczych.

Minimalne wymagania techniczne do monitora

Wielkość i rodzaj ekranu 32" IPS – podświetlenie krawędziowe LED
Rozdzielczość natywna panelu (min) 1920 x 1080 px
Obsługiwana rozdzielczość 4096 x 2160
Jasność 450 cd/m2
Poziom refleksyjności panelu minimum 28%
Możliwość pracy 24h/7 TAK
Obsługiwana orientacja Poziom, Pion
Wejścia wideo 1x DisplayPort ; 2x HDMI
MediaPlayer USB - obsługa rozdzielczości UHD
- wsparcie kodeka HEVC H.265
- wsparcie formatów MPG, MP4, TS, LPCM, MP3, AAC, WMV
Zasilany port USB USB (10W)
Złącza sterowania LAN, RS232
Wbudowane czujniki: 3 czujniki temperatury z możliwością programowania działań, oraz czujnik natężenia oświetlenia w otoczeniu
Wbudowane głośniki:2x 5W

Inne funkcjonalności

- Kalibracja kolorymetryczna, polegająca na możliwości zapisania wewnętrznej tablicy LUT monitora za pomocą oprogramowania tego samego producenta co monitor.
- Kalibracja sprzętowa zawierająca, możliwość kalibracji koordynatów chromatycznych bieli, krzywej transferu elektro optycznego, barwy niebieskiej, zielonej i czerwonej w zakresie zgodności kolorymetrycznej.
- Aktywny system chłodzenia awaryjnego za pomocą wentylatorów
- Możliwość sklonowania ustawień monitora do pamięci USB
- Sterowanie monitorem za pomocą przeglądarki www, lub przez dedykowane oprogramowanie producenta

WYMAGANIA OGÓLNO-FUNKCJONALNE DO SYSTEMU ZARZĄDZANIA WIDEO (VMS)

1. **Parametry minimalne i wymagania funkcjonalne dla systemu zarządzania bezpieczeństwem**

1.1. Oferowany system musi spajać w sposób logiczny i przez wspólny interfejs użytkownika co najmniej 4 własne moduły: zarządzanie źródłami video, kontrola dostępu, rozpoznawania tablic rejestracyjnych, rozpoznawanie twarzy.
1.2. Oferowany system musi być otwarty, z ogólnodostępnym Software Development Kit (SDK). Funkcjonalność ta powinna umożliwiać w razie potrzeby integrację z dowolnymi kamerami CCTV IP, zewnętrznymi systemami alarmowymi i kontroli dostępu.
1.3. System musi oferować możliwość integracji wykorzystując protokół OPC. Dopuszcza się stosowanie zewnętrznych modułów integracji OPC, o ile są.
1.4. Otwartość systemu musi umożliwiać wykorzystanie będących w powszechnej dystrybucji stacji klienckich, serwerów urządzeń infrastruktury sieci oraz pamięci masowych.

1.5. System musi posiadać możliwość dekodowania strumieni H.264 oraz H.265 po stronie karty graficznej, z możliwością przydzielenia dedykowanych kart do poszczególnych kodeków.
1.6. System musi obsługiwać kodeki MJPEG, MPEG4, H.264, H.265, MxPEG.
1.7. System musi być oprogramowaniem pracującym w architekturze klient-serwer. Część serwerowa musi odpowiadać za wszystkie procesy związane z rejestracją i zarządzaniem oraz udostępnianiem danych do stacji klienckich, natomiast część kliencka ma odpowiadać jedynie za pobieranie i wizualizowanie tych danych. Serwer platformy może zostać uruchomiony na pojedynczym serwerze lub na kilku serwerach w rozproszonej architekturze. Cała komunikacja między serwerem a aplikacją kliencką oparta jest na standardowym protokole TCP/IP wraz z możliwością uruchomienia szyfrowania.
1.8. VMS musi zapewniać elastyczność i możliwość integracji, dlatego musi obsługiwać wideo dekodery (wideoserwery przetwarzające analogowe sygnały wideo na strumienie cyfrowe) oraz kamery IP, różnych producentów, w tym: AXIS, ACTI, ARECONT, AVIGILON, AIRLIVE, AVER, AVTECH, BASLER, CANON, D-LINK, DAHUA, DYNACOLOR, ENEO, FLIR, GANZ, FOSCAM, GEOVISION, HANWHA, HIKVISION, HUNT, IQEYE, JVC, LEICA, LG, LEVELONE, MOBOTIX, MILESIGHT, MOXA DECODERS, MOXA I/O, PELCO, PANASONIC, SAMSUNG, SONY, SUNELL, TOA, TVT, UNIVIEW, UTC, VIVOTEC, YUDOR, ZAVIO, Y-CAM. System musi umożliwiać podgląd jak i rejestracje urządzeń podłączonych po USB (kamery inspekcyjne, kamery web, skanery, kamery termowizyjne itp.) bez limitu kanałów.
1.9. System VMS w celu zapewnienia elastyczności musi umożliwić natywną integrację z popularnymi systemami kontroli dostępu, w tym przynajmniej z Roger RACS 5, Gallagher Command Centre, Paxton. Integracja musi umożliwiać wyszukiwanie nagrań wykorzystując dane zapisane po stronie kontrolera kontroli dostępu. System musi umożliwić tworzenie wewnętrznych i zewnętrznych zdarzeń (automatyczne zakładki wideo, pop-up, email, żądania HTTP, wyzwalanie wyjść alarmowych, presetów itp) na podstawie zdarzeń z kontroli dostępu. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz
z systemem. W celu scentralizowania i usprawnienia pracy systemu, VMS musi umożliwiać natywną integrację z popularnymi systemami alarmowymi, w tym przynajmniej z SATEL INTEGRA. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem. Bez limitu ilości elementów kontroli dostępu oraz systemu alarmowego.
1.10. System VMS musi umożliwiać wsparcie dla kamer obsługujących ONVIF. Integracja ONVIF musi umożliwiać obsługę detekcji ruchu, wejść/wyjść alarmowych, analizy obrazu, zapisu i synchronizacji nagrań z kart pamięci (tak zwane EDGE recording lub ANR – Automatic Network Replenishment) jeśli kamera jest zgodna z odpowiednim profilem ONVIF
1.11. Aplikacja serwerowa systemu musi posiadać wbudowany silnik analizy obrazu, bazujący na sieciach neuronowych i umożliwiać uruchomienie takiej analizy obrazu na dowolnym strumieniu wideo (RTSP, MJPEG, MxPEG, ONVIF) jak również do już zarejestrowanego materiału (pliki AVI). Analiza obrazu powinna umożliwiać filtrowanie zdarzeń na podstawie wykrytych obiektów, lista powinna zawierać przynajmniej następujące obiekty: samochód osobowy, bus, ciężarówka, łódź, człowiek, motocykl, rower, zwierzę. Licencja za analizę obrazu nie powinna być przypisana na stałe dla danego kanału, powinna umożliwiać dowolne przenoszenie w ramach strumieni wideo dostępnych w systemie.
1.12. System musi posiadać możliwość zliczania dowolnych zdarzeń z analizy obrazu, wejść alarmowych i czujników zewnętrznych. Zliczanie powinno odbywać się na dowolnej liczbie

kamer i urządzeń z możliwością sumowania i odejmowania. System musi umożliwiać tworzenie zdarzeń i procedur na podstawie wartości poszczególnych liczników.
1.13. System musi umożliwiać tworzenie automatycznych zakładek na materiale wideo. Zakładki powinny być tworzone automatycznie, wraz z automatycznym opisem (rodzaj zdarzenia, numer zdarzenia, kamera, lokalizacja) jako wynik analizy obrazu (zarówno na kamerze jak i po stronie serwera), detekcji ruchu, wartości licznika, zdarzeń systemowych, danych POS, komend CGI i żądań http z aplikacji zewnętrznych (wymagane w celach integracji i aby zapewnić elastyczność systemu). Jeśli funkcjonalność tworzenia zakładek wymaga dodatkowej licencji, musi być ona dostarczona wraz z systemem.
1.14. System musi umożliwiać rejestrowanie strumieni wideo wysyłanych na żywo z urządzeń Android i iOS wraz z ich położeniem przesłanym na podstawie GPS. Dopuszcza się stosowanie dedykowanej aplikacji po stronie urządzenia do wysyłania obrazu. Funkcjonalność powinna być zintegrowana i dostarczona wraz z aplikacja serwerową i powinna być dostępna dla wszystkich kanałów dostępnych dla danej licencji.
1.15. System musi wspierać koncepcję federacji, czyli wiele niezależnych instalacji VMS może być połączonych w jeden duży wirtualny system scentralizowanego monitorowania, raportowania i zarządzania alarmami jak również zarządzania użytkownikami (tworzenie, przydzielanie ról i uprawnień, oraz monitoring zajętości pasma sieciowego i zasobów serwera).
1.16. System VMS i jego komponenty (aplikacja serwerowa, konsola, aplikacja kliencka) musi posiadać możliwość pracy w środowisku wirtualnym. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.
1.17. System VMS musi umożliwiać tworzenie interaktywnych przycisków umożliwiających wywoływanie komend CGI, wysyłanie żądań http, resetowanie liczników, generowanie alarmów, uzbrajanie/rozbrajanie systemów alarmowych, wyzwalanie wyjść alarmowych. System musi również umożliwiać inne działanie dane przycisku
w zależności od zmiennych przydzielanych przez system (np. inne działanie przycisku w zależności poziomu temperatury podanym przez czujnik temperatury
w serwerowni). System VMS musi umożliwiać stworzenie dowolnej ilości przycisków bez wymogu dodatkowych licencji.
1.18. Licencja na system VMS nie powinna być przypisana do specyfikacji sprzętowej serwera
i umożliwiać przenoszenie na inne serwery bez ingerencji producenta.
1.19. System musi umożliwiać podłączenie 250 klientów (android, iOS, aplikacja kliencka, przeglądarka) w tym samym momencie. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.
1.20. System VMS musi posiadać funkcję audytu, która będzie rejestrowała w osobnej, szyfrowanej bazie danych, wszystkie zdarzenia i akcje podejmowane przez dowolnego użytkownika na stacji klienckiej jak i aplikacji serwerowej.
1.21. Aby zapewnić łatwość integracji z zewnętrznymi systemami i czujnikami, system musi posiadać wbudowany tak zwany sniffer danych wysyłanych na port COM lub wybrany port sieciowy. Sniffer musi umożliwiać filtrowanie przesyłanych danych w celu wyodrębnienia ciągów znaków i używania ich jak zmiennych w systemie (dane liczbowe, np. z czujników, wag drogowych) jak również opisów do automatycznych zakładek. System musi umożliwiać tworzenie zdarzeń (wysyłanie email, okna pop-up, notyfikacje push) na podstawie zdefiniowanych ciągów znaków. Jeśli ta funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.
1.22. VMS będzie działał na standardowych systemach operacyjnych Windows i różnych mobilnych systemach operacyjnych dla platform opartych na aplikacjach mobilnych.

1.23. VMS musi obsługiwać funkcję multicastu, a także możliwość unicastu dla każdego urządzenia peryferyjnego kamery w wielu instancjach jednocześnie.
1.24. Producent systemu VMS musi umożliwiać świadczenie wsparcia (aktualizacji, poprawek) dla systemu na okres minimum 10 lat.

2. **Federacja: Obsługa zdalnych systemów**

2.1. Funkcja federacji zezwala na połączenie wielu niezależnych systemów VMS (systemów sfederowanych) w większy system wirtualny (Federację). Umożliwia to globalne monitorowanie wielu niezależnych systemów VMS producenta.
2.2. VMS musi działać w architekturze federacyjnej umożliwiającej każdemu upoważnionemu użytkownikowi bezproblemowy dostęp do zasobów systemowych (takich jak wideo na żywo/nagrane) podłączonych do dowolnego serwera sieciowego.
2.3. Architektura federacyjna umożliwi również scentralizowaną administrację serwerów aplikacji, aplikacji klienckich i koderów/aparatów cyfrowych w celu aktualizacji oprogramowania, oprogramowania układowego, dystrybucji alarmów i alertów oraz tworzenia kopii zapasowych danych konfiguracyjnych.
2.4. Funkcja federacji musi unifikować wiele odrębnych (logicznie, lub geograficznie) systemów bezpieczeństwa.
2.5. Federacja musi obsługiwać alarmy i kamery.
2.6. System musi umożliwiać nagrywanie dowolnego ekranów innych stacji klienckich i serwerów wraz z obsługa nagrywania ściany wizyjnej.

3. **Integracja z Microsoft Active Directory**

3.1. Platforma VMS pozwala na bezpośrednie połączenie z jednym lub wieloma serwerami Microsoft Active Directory poprzez Role AD. Integracja z Active Directory umożliwia synchronizację informacji serwera Active Directory.
3.2. Jeśli zezwolono, Active Directory zarządza logowaniem użytkowników do aplikacji klienckiej platformy VMS poprzez poświadczenia użytkownika Windows. Logowanie do platformy VMS wykorzystuje opcje zarządzania hasłami i autoryzacji Active Directory. Dodawanie, usuwanie lub zawieszanie konta użytkownika Windows w Active Directory skutkuje utworzeniem, usunięciem lub wyłączeniem odpowiedniego konta użytkownika w platformie VMS.

4. **Praca awaryjna (Failover), czuwanie (Standby), bezpieczeństwo.**
   4.1. System musi obsługiwać własne opcje pracy w przypadku wystąpienia awarii (failover).
   4.2. System musi umożliwiać obsługę serwerów centralnych (standby) działający jako serwery zastępcze pracujące w trybie czuwania. W przypadku awarii dowolnego serwera w systemie, serwer centralny przejmie wszystkie połączenia oraz ustawienia takiego serwera. Przejęcie może nastąpić w czasie krótszym niż 2 minuty. Nie powinno to wymagać ingerencji użytkownika. System powinien umożliwiać konfigurację czasu po jakim serwer standbay określa awarię serwera VMS. System musi umożliwiać redundancję „n do 1", jak również „1 do n". System musi umożliwiać stworzenie minimum 4 serwerów redundantnych. Przejęcie przez serwer standbay musi obywać się kaskadowo. Jeśli taka funkcjonalność wymaga dodatkowej licencji, powinna być ona dostarczona wraz z systemem.
   4.3. Zapasowy serwer centralny powinien mieć możliwość zachowania bazy danych konfiguracji zsynchronizowanej z głównym serwerem centralnym.
   4.4. System VMS musi umożliwiać tworzenie oddzielnych baz danych dla zdarzeń, użytkowników, nagrań oraz dla audytu systemu wraz z oddzielnym sposobem szyfrowania.
   4.5. System musi automatycznie szyfrować wszystkie bazy danych (również bazę nagrań), jak również dodatkowo zabezpieczać je hasłem.

4.6. System musi wykorzystywać tunelowanie HTTPS SSL/TLS, w celu zabezpieczania komunikacji serwer-serwer, serwer-klient, serwer-kamera nie tylko przy użyciu hasła, ale również szyfrowania całej transmisji (zabezpieczanie nie tylko komunikatu, ale również komunikacji, aby zminimalizować ryzyko ataku man-in-the-middle)
4.7. VMS musi wykorzystywać czasowe tokeny do zestawiania połączeń sieciowych, aby zabezpieczyć system przed atakami DoS.
4.8. System musi umożliwiać tworzenie własnych polityk haseł użytkowników, definiujących długość hasła, ilość prób logowania, ilość znaków specjalnych.
4.9. System musi umożliwiać definiowanie co do minuty długości archiwum do jakiego dostęp ma dany użytkownik, bez względu na to jak długie archiwum znajduje się na serwerze.
4.10. System musi dokumentować wszystkie zmiany związane z użytkownikiem w aplikacji
i podłączonych urządzeniach peryferyjnych ze środowiskiem aplikacji.

5. **Aplikacja Kliencka**

5.1. Aplikacja kliencka musi zapewnić interfejs użytkownika dla konfiguracji i monitorowania
w dowolnej sieci, dostępnej lokalnie lub poprzez połączenie zdalne.
5.2. Wszystkie aplikacje muszą posiadać mechanizm autoryzacyjny, który weryfikuje użytkownika. Dzięki temu administrator (posiadający wszelkie prawa i przywileje) może zdefiniować określone prawa dostępu dla każdego użytkownika w systemie.
5.3. Logowanie do aplikacji klienta musi przebiegać poprzez konta i hasła systemu przechowywane lokalnie lub poprzez uwierzytelnienia użytkownika Windows, gdy integracja z Active Directory jest włączona.
5.4. Aplikacja kliencka musi być dostępna w języku polskim.
5.5. Aplikacja kliencka musi mieć możliwość zablokowania powłoki Windows, aby uniemożliwić zamknięcie czy zminimalizowanie aplikacji bez podania hasła nadanego przez administratora.
5.6. Aplikacja kliencka musi posiadać interfejs do wygodnego przeglądania nagrań ze wszystkich wyświetlonych kamer (od 1 do 100 jednocześnie). Interfejs powinien posiadać oś czasu obrazującą obecność nagrań, jak również zaznaczone okresy detekcji ruchu (oddzielne kolory dla detekcji po stronie serwera jak i po stronie kamery), nagrywania ciągłego, nagrywania po zdarzeniu z analizy obrazu (zarówno z kamery jak i z serwera).
5.7. Aplikacja kliencka musi posiadać interfejs do eksportowania nagrań z 72 kamer jednocześnie. Użytkownik powinien mieć możliwość eksportu nagrań z wielu kamer w postaci pojedynczych plików, jak również w postaci jednego pliku mozaikowego złożonego z nagrań wszystkich wyświetlonych kamer (wsparcie dla rozdzielczości 8K dla pliku wyjściowego).
5.8. System będzie w stanie pobierać nagrane wideo na podstawie kryteriów wyszukiwania użytkowników, w tym kombinacji:

- identyfikator referencyjny kamery,
- data i godzina nagrania z kamery,
- zaznaczenie obszaru wokół interesującego obiektu w celu ustalenia, kiedy obiekt pojawił się w scenie,
- zdarzenia alarmowe,
- zakładki dodawane automatycznie lub ręcznie przez użytkownika,
- alfanumeryczny ciąg metadanych (np. numer transakcji nagrany za pomocą wideo
z innych systemów, numery tablic rejestracyjnych, kody kreskowe, dane z wag itp.).

5.9. VMS zbuduje pojedynczy, złożony plik do eksportu zawierający sekwencję wybranych nagrań z kamer, w których materiał musi być zbudowany z wielu sekwencji, kamer i pól widzenia
w czasie.
5.10. Aplikacja musi oferować interfejs do wyszukiwania ciągów znaków odbieranych i filtrowanych przez sniffer po stronie serwera.
5.11. Tam, gdzie pozwalają na to zasady i przepisy, system będzie miał możliwość integracji 1- lub 2-stronnej komunikacji głosowej w celu obsługi funkcji wideo w różnych lokalizacjach w zależności od potrzeb użytkownika.

6. **Mapy**

System musi posiadać zintegrowane narzędzie do edycji i tworzenia map rozmieszczenia elementów technicznego systemu zabezpieczeń. Graficzny interfejs mapy musi spełniać co najmniej następujące wymagania:

6.1. Wyświetlanie wielu map dla jednego oraz dla wielu obszarów
6.2. Wyświetlanie map jako warstw
6.3. Wyświetlanie podkładów mapowych w postaci map GIS np. OpenStreetMap, Google Map, TomTom. Jeśli funkcjonalność wymaga licencji musi być ona dostarczona wraz z systemem, dla minimum 10 map GIS
6.4. Wyświetlanie podkładów mapowych w postaci bitmap
6.5. Przełączanie się pomiędzy mapami poprzez aktywne przyciski, również między mapami GIS i bitmapami
6.6. Wyświetlanie na mapie aktywnych ikon urządzeń w systemie,
6.7. Wyświetlanie na mapie aktywnych obszarów obserwacji kamer stacjonarnych w systemie
6.8. Wyświetlanie na mapie aktywnych ikon urządzeń powiązanych z alarmami takich jak status drzwi z kontroli dostępu, czujki ruchu, bariery podczerwieni. Wraz z możliwością definiowania własnych ikon i ich kolorów i stanów.
6.9. Centralne zarządzanie mapami.

7. **Otwarta architektura**

7.1. System musi być neutralny w stosunku do producentów urządzeń technicznych systemów bezpieczeństwa dostępnych na rynku i umożliwiać ich integracje udostępniając Software Development Kits (SDK), Driver Development Kits (DDK), Web Service SDK.
7.2. System musi posiadać możliwość dodania plug-inów integrujących systemy zewnętrzne, takie jak:
7.2.1. Analityka wideo
7.2.2. Zewnętrzne systemy firm trzecich
7.3. Wszystkie kamery podłączone do VMS muszą być sterowane przez dowolne urządzenie wejściowe. Obejmuje to między innymi mysz, joysticki, panele sterowania, ekran dotykowy, urządzenia mobilne lub urządzenia wejściowe z klawiaturą.

8. **Inne**

8.1. System musi umożliwiać tworzenie i zarządzanie ścianą wideo, poprzez zastosowania stacji komputerowych typu desktop i dołączonych monitorów, zamiast dedykowanego rozwiązania dla ścian wideo. System musi umożliwiać stworzenie minimum 10 niezależnych ścian wizyjnych. Każda ze ścian wizyjnych musi obsługiwać minimum 9 monitorów. Jeśli funkcjonalność wymaga dodatkowej licencji powinna być ona dostarczona wraz z systemem.
8.2. Architektura platformy VMS powinna umożliwiać pełną skalowalność, i ma umożliwiać rozbudowę systemu o:
8.2.1. Co najmniej 1000 serwerów rejestracji i zarządzania
8.2.2. Co najmniej 500 stacji klienckich
8.2.3. Co najmniej 15000 kamer

8.2.4. Co najmniej 15000 modułów wejść/wyjść alarmowych
8.3. System musi posiadać usługę nieprzerwanie monitorującą pracę i stan usług serwerów. Usługa monitorująca musi działać w środowisku Windows i być automatycznie uruchamiana podczas startu systemu niezależnie od tego czy użytkownik jest zalogowany czy nie.
W wypadku wystąpienia błędu lub awarii usługa monitorująca musi restartować usługę w której wystąpił błąd, a w ostateczności uruchomić ponownie serwer/komputer jeśli nie jest w stanie uruchomić ponownie usługi. Usługa powinna zapisywać zdarzenia w wydzielonej, szyfrowanej i zabezpieczonej hasłem bazie danych.
8.4. System musi posiadać ramy usług konserwacji i naprawy wsparcia, aby zapewnić integralność systemu, bezpieczeństwo i ciągłość działania.

Wymaga się aby system VMS wdrażała firma posiadająca aktualny certyfikat producenta sprzętu z zakresu instalacji oraz uruchomienia. Zapewni to lepszą jakość wykonanej pracy oraz umożliwi ewentualne wsparcie producenckie na etapie uruchamiania systemu oraz szkolenia personelu z obsługi systemu.

Wskazane jest aby Wykonawca dokonał wizji lokalnej w miejscach opisanych w Specyfikacji oraz uzyskał na swoją odpowiedzialność i ryzyko wszelkie istotne informacje, które mogą być przydatne do przygotowania oferty. Wizja lokalna winna być wykonana na koszt własny Wykonawcy.