*Wymagania funkcjonalne oprogramowania VMS*

Oprogramowanie spełniające wszystkie kryteria: **GANZ CORTROL GLOBAL (wer.1.26.0)**

1. **Informacje ogólne:**

Oprogramowanie do zarządzania systemem wideo nadzoru powinno spełniać standardy profesjonalnej platformy VMS (Video Management Software) klasy ENTERPRISE o dużej skalowalności i wydajności. Ma zapewniać niewielkie obciążenie zasobów CPU i GPU w stosunku do ilości urządzeń podłączonych do systemu. System VMS ma zapewniać integrację z różnymi modelami urządzeń (m.in. kamery, enkodery, moduły wejść/wyjść) wielu producentów. Oprogramowanie powinno posiadać funkcje i moduły wspomagające nadzór wizyjny, m.in.:

* analityka wideo VCA,
* analityka AI,
* biometryczna identyfikacja twarzy o wysokiej skuteczności,
* odczytywanie numerów tablic rejestracyjnych,
* inteligentne wyszukiwanie nagrań.

Oprogramowanie VMS powinno być zoptymalizowane do pracy w środowisku Microsoft Windows Server 2016/2019 oraz Windows 10/11. Serwer centralny ma wspierać pracę w środowisku wirtualnym.

1. **Licencjonowanie oprogramowania VMS:**

Oprogramowanie musi być licencjonowane w zależności od ilości dostępnych kanałów wideo i powinno zapewniać uruchomienie i stabilną obsługę dowolnej ilości kanałów wideo w obrębie jednego systemu z możliwością dowolnego rozproszenia tych kanałów na poszczególne jednostki serwerowe. Ponadto, oprogramowanie musi gwarantować:

1. licencjonowanie bez ograniczeń terminowych, czyli tzw. licencja dożywotnia uprawniająca do bezterminowego korzystania ze wszystkich funkcjonalności objętych nominalnie zakresem zakupionej licencji.
2. możliwość łączenia z kamerami oraz rejestratorami NVR z poza sieci LAN
3. możliwość aktywacji licencji i pracy systemu w środowisku wirtualnym.
4. nieograniczoną ilość połączeń zdalnych klientów do jednostki/jednostek serwerowych
5. możliwość subskrypcji pozwalającej na korzystanie z aktualizacji i najnowszych wersji oprogramowania
6. **Funkcjonalność oprogramowania VMS:**

**Aplikacja Nagrywająca**

Z uwagi na zapewnienie stabilnej i wydajnej pracy systemu, oprogramowanie VMS musi posiadać niezależny komponent (aplikację serwerową) służącą do realizacji nagrywania strumieni wideo, audio, tekstowych z poszczególnych urządzeń IP. Aplikacja nagrywająca musi spełniać warunek pracy w trybie usługi (Windows service mode). Komunikacja pomiędzy aplikacją serwerową i kliencką musi być szyfrowana algorytmem min. 265bit AES.

**Obsługa wideo musi posiadać następujące możliwości:**

1. obsługa kodeków H265, H.264, MPEG4, MJPEG, JPEG, MxPEG,
2. obsługa transportu wideo RTSP, HTTP, natywnie,
3. konfigurowalny stopień kompresji, rozdzielczość, ilość klatek na sekundę, wielkość strumienia (bitrate),
4. nadrukowywanie informacji tekstowych na wideo, np. POS,
5. wsparcie sprzętowe GPU dla strumieni H.264 i H.265,
6. nagrania muszą być szyfrowane minimum algorytmem 265bit AES,
7. zmianę właściwości obrazu (jasność/nasycenie/kontrast/ostrość/balans bieli/ekspozycja).

**Obsługa urządzeń IP powinna spełniać podane warunki:**

1. wsparcie szerokiego zakresu urządzeń IP, w tym kamer, enkoderów, rejestratorów, czujników ruchu, modułów wejść/wyjść, kontroli dostępu,
2. wykrywanie urządzeń sieciowych automatycznie poprzez auto-skanowanie sieci,
3. indywidualna oraz grupowa konfiguracja kamer IP,
4. obsługa ogólnych sterowników ONVIF, RTSP, PSIA, HTTP, HTTPS, USB CAMERA, WASAPI,
5. sterowanie wejść/wyjść oraz audio wbudowanych w urządzenia wideo,
6. obsługa strumieni wideo pochodzących z urządzeń mobilnych Android i iOS wyposażonych w kompatybilną aplikację mobilną,
7. obsługa nagrywania brzegowego (EDGE) z urządzeń zgodnych z ONVIF G,
8. obsługa urządzeń typu – Interaktywny link / pulpit zdalny.

**Archiwizacja danych powinna zapewniać:**

1. indywidualną replikację kanałów wideo z programowanym harmonogramem replikowania danych na wskazane nośniki i zasoby sieciowe,
2. nagrywanie w trybie ciągłym, detekcji ruchu, alarmowym na podstawie alarmów z analityki VCA, urządzeń zewnętrznych oraz innych akcji/scenariuszy definiowanych w systemie,
3. możliwość nagrywania co najmniej dwóch strumieni dostępnych w urządzeniu i odtwarzania optymalnego strumienia w zależności od trybu odtwarzania (np. pełnoekranowy, podział ekranu)
4. szyfrowanie bazy danych archiwalnych metodą nie gorszą niż AES-256bit,
5. dodawanie znaczników z komentarzem i poziomem istotności (tzw. bookmark) na osi czasu zarówno w trybie LIVE jak i podczas odtwarzania archiwum. Treść komentarza ma służyć ułatwieniu wyszukiwania żądanych nagrań,
6. przypisanie dedykowanego archiwum (tzn. wskazany nośnik lokalny lub zasób sieciowy) jak również zdefiniowanie retencji danych (okres) oraz rozmiaru archiwum (GB) indywidualnie dla każdego kanału wideo w systemie,
7. archiwizację audio oraz danych tekstowych (np. POS) równolegle z danymi wideo z zachowaniem synchronizacji czasowej wszystkich danych,
8. nagrywanie brzegowe EDGE zgodne z urządzeniami obsługującymi protokół ONVIF Profile G, polegające na wykorzystaniu lokalnej pamięci urządzenia do tymczasowego nagrywania w sytuacji utraty komunikacji z urządzeniem, oraz automatycznego uzupełnienia brakującego archiwum w bazie centralnej po odzyskaniu komunikacji z urządzeniem,
9. nielimitowana rozdzielczość zapisywanych strumieni na serwerze,
10. zabezpieczenie dowolnego zakresu materiału z archiwum przed napisaniem lub usunięciem,
11. ręczne usunięcie dowolnego zakresu materiału z archiwum (fizycznie z dysków), wymagające dodatkowych uprawnień od użytkownika.

**Opcje nagrywania powinny umożliwiać:**

1. definiowanie profili nagrywania określających tryb oraz parametry nagrywania dla poszczególnych kanałów,
2. określanie czasu nagrywania pre-alarm (przed wystąpieniem alarmu) oraz post-alarm (po wystąpieniu alarmu),
3. automatyczne aktywowanie wskazanych profili nagrywania w zależności od rodzaju występujących zdarzeń,
4. ręczne wyzwalanie określonych profili nagrywania przez operatora, np. napad,
5. niezależne definiowanie indywidualnych limitów archiwum (ilość dni, rozmiar w GB) dla każdego strumienia wideo,
6. tworzenie harmonogramów nagrywania w oparciu o dni tygodnia oraz kalendarze użytkownika,
7. programowanie harmonogramów do automatycznego czyszczenia archiwum i porządkowania indeksów.

**Funkcja Watchdog powinna spełniać poniższe wymagania:**

1. zabezpieczenie aplikacji przed różnymi typami nieoczekiwanych zjawisk mogących powodować zatrzymanie lub zakłócenie prawidłowej pracy, poprzez wymuszanie restartu usługi lub jednostki serwerowej, jeśli zajdzie taka konieczność,
2. obsługę planowanych wg harmonogramu restartów jednostek serwerowych,
3. podejmowania restartów na podstawie całościowego monitorowania statusu aplikacji oraz komponentów systemu,
4. konfiguracja indywidualna dla każdej jednostki serwerowej,
5. przechowywanie logów z aktywności usługi,
6. aktywnej komunikacji pomiędzy innymi watchdogami w systemie (między rejestratorami i serwerami awaryjnymi), w celu monitorowania stanu serwerów i wymuszenia pracy awaryjnej.

**Detekcja ruchu powinna zapewniać:**

1. obsługę detekcji ruchu po stronie kamery, która działając na surowym (nieskompresowanym) obrazie wideo daje lepsze rezultaty i ponadto nie obciąża serwera,
2. obsługę programowej detekcji ruchu po stronie serwera w trybie wysokiej wydajności, czyli z analizą wyłącznie klatek kluczowych, co obniża obciążenie procesora i zajętość pamięci, zapewniając zredukowaną skuteczność,
3. obsługę programowej detekcji ruchu po stronie serwera w trybie wysokiej skuteczności, czyli z analizą pełnego strumienia wideo zapewniającą maksymalną skuteczność, zalecaną do miejsc gdzie zachodzi konieczność detekcji krótkotrwałych zdarzeń, trwających poniżej 1 sek,
4. obsługę metadanych zwierające koordynaty wystąpienia detekcji ruchu w celu inteligentnego wyszukiwania materiałów wideo.

**Programowa analityka po stronie serwera musi zapewniać:**

1. analizę wideo z uwzględnieniem predefiniowanych filtrów i klasyfikatorów,
2. wyświetlanie meta danych (m.in. ramki alarmowe otaczające obiekty, trasa poruszania się obiektu, parametry i klasa obiektu) na obrazie wideo jak i liczniki czy też dane diagnostyczne ułatwiające konfigurację,
3. rozróżnianie co najmniej pięciu różnych klas obiektów (np. człowiek, rower, samochód, motocykl, samolot, autobus, pociąg, sam. ciężarowy, łódź, kot, pies, koń),
4. możliwość uruchomienia analityki bez wymaganego dodatkowego hardware/serwera,
5. zliczanie wybranej klasy obiektów w określonych kierunkach, co najmniej 5 liczników na jednym kanale wideo,
6. detekcję zatrzymania się wybranej klasy obiektu w zabronionej strefie,
7. detekcję pozostawionych przedmiotów,
8. wykrycie wejścia oraz wyjścia określonej klasy obiektu z monitorowanej strefy,
9. detekcję pojawienia się lub zniknięcia obiektu z monitorowanej strefy,
10. wyszukiwanie zdarzeń analizy wideo po dowolnej klasie obiektu, regule czy strefie,
11. silnik analityczny wykorzystujący sieci neuronowe CNNE,
12. dedykowaną bazę danych dla wyników analizy wideo,
13. wsparcie dla GPU NVIDIA dla obliczeń wykonywanych w ramach analizy wideo,
14. możliwość ustawienia parametru czasu obiektu dla algorytmów obecności i nieobecności.

**System musi zapewniać możliwość tworzenia scenariuszy automatycznego działania w następującym zakresie:**

1. wysyłanie powiadomień e-mail zawierających takie dane jak czas wystąpienia zdarzenia, zdjęcie alarmowe, źródło alarmu. Konfiguracja musi pozwalać na wprowadzenie wielu różnych serwerów SMTP (dla różnych adresów e-mail),
2. wysyłanie powiadomień poprzez uruchomienie aplikacji zewnętrznych, np. z użyciem telnet,
3. tworzenie indywidualnych czasowych harmonogramów aktywności dla każdego scenariusza,
4. tworzenie globalnych scenariuszy wykorzystujących zdarzenia alarmowe z dowolnego serwera i wykonujących akcję na innym dowolnym serwerze,
5. tworzenie kombinacji wielu zdarzeń z warunkiem logicznym wyzwalającym akcję,
6. wykonywanie akcji z predefiniowanym opóźnieniem (czasem zwłoki) po wystąpieniu zdarzenia,
7. agregacja zdarzeń i wykonanie akcji dopiero po przekroczeniu określonej ilości skumulowanych zdarzeń,
8. jedno zdarzenie musi mieć możliwość wyzwolenia dowolnej liczby wybranych akcji.

**Obsługa audio powinna działać w poniższym zakresie:**

1. odbiór dźwięku z urządzenia oraz nadawanie dźwięku do urządzenia (transmisja dwukierunkowa),
2. obsługa zewnętrznych źródeł dźwięku typu mikrofon podłączony do jednostki klienckiej,
3. wysłanie lokalnego pliku audio wprost do odtworzenia na wyjściu audio kamery.

**System musi zapewniać możliwość organizacji zasobów w następującym zakresie:**

1. podział zasobów całego systemu na logiczne partycje (podsystemy), do których przypisane mogą być wybrane kanały wideo, wybrani użytkownicy oraz sub-administratorzy,
2. sub-administratorzy powinni być uprawnieni do zarządzania przypisanym podsystemem w zakresie użytkowników oraz nadawania im praw dostępu do poszczególnych kanałów.

**System musi zapewniać obsługę klastrową Failover w poniższym zakresie funkcjonalności**

1. działanie failover bez wymaganych dodatkowych licencji,
2. nieograniczona ilość klastrów failover oraz węzłów (serwerów failover),
3. działanie failover w układzie jeden-do-wielu oraz wiele-do-jednego,
4. automatyczne uruchomienie procedury failover po wykryciu awarii serwera należącego do klastra wraz z możliwością definiowania czasu opóźnienia startu procesu failover,
5. możliwość ręcznego uruchomienia procesu failover na potrzeby prac konserwacyjno-serwisowych serwerów,
6. bieżące monitorowanie statusu serwerów failover.

**System powinien zapewniać automatyczne kierowanie ruchu sieciowego zgodnie z poniższymi wytycznymi:**

1. łączenie się użytkowników do zasobów systemowych poprzez centralny serwer zarządzający ruchem (routing TCP/IP), bez konieczności wprowadzania adresów poszczególnych serwerów nagrywających,
2. zapewnienie przezroczystej infrastruktury systemu dla użytkownika,
3. obsługa komunikacji w trybie Multicast na poziomie serwerów nagrywających.

**Grupowanie zasobów systemu powinno być możliwe w następującym zakresie:**

1. serwery nagrywające.
2. użytkownicy systemu.
3. urządzenia (kamery, enkodery, rejestratory, moduły wejść/wyjść, itp.),
4. kanały wideo,
5. e-mapy synoptyczne,
6. szablony i ekranowe układy obrazów,
7. ściany monitorów video-wall,
8. przyciski użytkownika.

**Zarządzanie użytkownikami systemu musi umożliwiać**

1. przypisanie użytkownikowi: identyfikatora, hasła, adresu e-mail, przynależności do wybranej organizacji w systemie, priorytetu w sterowaniu PTZ,
2. definiowanie wymaganego poziomu siły hasła oraz okresu ważności hasła,
3. nadawanie użytkownikowi uprawnień w zakresie: serwerów, sieci, urządzeń, kanałów, e-map synoptycznych, przycisków użytkownika, szablonów widoków ekranowych, ścian monitorów (wideo wall),
4. przynależność do wybranej grupy lub wielu grup użytkowników,
5. tworzenie nieograniczonej ilości kont użytkowników systemu,
6. korzystanie z użytkowników oraz grup użytkowników Active Directory, LDAP,
7. automatyczna synchronizacja usuniętych oraz nowo utworzonych kont użytkownika w Active Directory,
8. logowanie przy pomocy protokołu OAuth 2.0,
9. blokowanie możliwości logowania po N próbach,
10. uwierzytelnianie dwuskładnikowe (dodatkowo email lub SMS),
11. kontrola dostępu do zasobów użytkowników i grup użytkowników w oparciu o harmonogram,
12. rozłączenie użytkownika po wyłączeniu, zmianie hasła, wygaśnięciu lub zresetowaniu tokena Oauth.

**System musi zapewniać ciągłe monitorowanie statusu i kondycji następujących komponentów:**

1. serwerów nagrywających, minimum: CPU na system, CPU na proces rejestratora, RAM, sieć,
2. urządzeń dodanych do systemu (kamery, rejestratory, enkodery, moduły wejść/wyjść, itp.),
3. sesje użytkowników wraz ze zdalnym monitorowaniem użytych zasobów jednostki klienckiej, jak dla serwera,
4. ściany monitorów (wideo wall),
5. usługi dodatkowe (np. czytanie tablic rejestracyjnych, identyfikacja twarzy),
6. usługa failover,
7. połączenia pomiędzy wszystkimi komponentami,
8. strumienie wideo,
9. zasoby dyskowe wraz ze statystykami archiwum,
10. aktualny status urządzeń powinien być dostępny w dedykowanym panelu monitorującym.

**Audyt systemu czyli dziennik logów musi spełniać następujące warunki:**

1. rejestrowanie zdarzeń zalogowania i wylogowania użytkownika, administrowania serwera i zmiany konfiguracji, uzyskania dostępu do podglądu live oraz do archiwum, rozłączenia i połączenia serwera,
2. generowanie raportów ze zdarzeniami w podziale na zdarzenia serwerów oraz zdarzenia użytkowników,
3. filtrowanie zdarzeń według okresu czasowego, typu zdarzenia, źródła zdarzenia serwer/użytkownik oraz komponentu,
4. eksportowanie raportów zdarzeń do pliku CSV, drukowanie,
5. możliwość podłączenia zewnętrznej baz danych (PostgreSQL, MySQL, Microsoft SQL Server) do przechowywania logów zdarzeń.

**Mapy synoptyczne powinny spełniać następującą funkcjonalność:**

1. określanie przynależności map do grup użytkowników oraz do organizacji,
2. importowanie map w postaci plików graficznych w formatach: JPEG, PNG, TIF, BMP, statyczny GIF o rozdzielczości do 8MPix,
3. dodawanie obiektów dynamicznych oraz przycisków użytkownika z możliwością indywidualnego zaprogramowania do pięciu różnych przełączalnych stanów sygnalizowanych odpowiednim tekstem, kolorem oraz ikoną (wielkość ikon i czcionki opisów konfigurowalna),
4. możliwość stosowania geo-map wraz z możliwością oznaczania elementów na niej takich jak kanały, przyciski,
5. geo-mapy oparte o darmowe rozwiązania dostarczania informacji oraz możliwość korzystania z własnego lokalnego/zdalnego serwera map,
6. posiadać miniatury obrazu na żywo przy podświetleniu kamery na mapach.

**Szablony i układy podziału ekranów wideo powinny zapewniać:**

1. tworzenie własnych widoków i układów podziału ekranu,
2. dzielenie ekranu maksymalnie na 20 kolumn lub 20 wierszy, łącznie do 100 okien wideo w jednym szablonie,
3. współdzielenie utworzonych własnych widoków w obrębie grupy użytkowników lub organizacji,
4. zapisywanie widoków wraz z presetami ustawień okna dla danego kanału, zoom, dewarping, strumień, itp.

**Przyciski użytkownika jako element interaktywny mapy synoptycznej powinny umożliwiać:**

1. ręczne wyzwolenie/uruchomienie określonej akcji spośród dostępnych w systemie (m.in. wysterowanie wyjścia alarmowego, uruchomienie presetu kamery PTZ, aktywacja określonego profilu/trybu nagrywania, powiadomienie, itp.),
2. określanie harmonogramów czasowych aktywności przycisku (blokowanie przycisku w okresach spoza harmonogramu).

**System powinien mieć możliwość automatycznej obsługi następujących zdarzeń:**

1. awaria/odłączenie dysku twardego,
2. pojawienie się błędów dysku twardego (uruchomienie trybu fallback),
3. aktywacja funkcji Failover,
4. detekcja ruchu z rozróżnieniem na stany: rozpoczęcie/trwanie/zakończenie,
5. błąd nagrywania, przywrócenie nagrywania,
6. timer (harmonogram),
7. aktywacja przycisku użytkownika,
8. zanik/przywrócenie strumienia wideo,
9. odebranie SMS’a,
10. aktywacja wejścia alarmowego urządzenia (kamery),
11. odebranie zdarzenia z urządzeń sieciowych po protokole MQTT,
12. wystąpienie zdarzenia analityki wideo VCA (zarówno po stronie urządzenia oraz serwera),
13. odebranie zewnętrznej komendy HTTP API,
14. odebranie dowolnej komendy z zewnętrznej integracji,
15. odebranie zdarzenia z OPC,
16. odebranie zdarzenia z zewnętrznego źródła (np. POS),
17. odebranie zdarzenia ze ściany wizyjnej video-wall,
18. spełnienie zaprogramowanego warunku wartości liczników (< ; = ; != ; >) zgodnie z PCRE Regular Expression.

**System powinien mieć możliwość automatycznego wykonania następujących akcji:**

1. alert (graficzny) dla wybranego strumienia wideo,
2. pop-up zawierający obraz z określonego kanału wideo, mapę synoptyczną lub widok ekranowy,
3. zapisanie do logów audytu,
4. aktywacja nagrywania zgodnie z określonym profilem/trybem,
5. aktywacja presetu PTZ,
6. włączenie/wyłączenie kanału,
7. włączenie/wyłączenie analityki wideo kanału,
8. dodanie znacznika w archiwum,
9. wyświetlenie zdarzenia na aplikacji mobilnej (dla określonych użytkowników),
10. eksport zdjęcia alarmowego na określony serwer FTP, do lokalnego folderu,
11. wysłanie wiadomości e-mail z załączonym zdjęciem alarmowym,
12. odtworzenie pliku audio do wyjścia audio we wskazanym urządzeniu (kamera, głośnik),
13. uruchomienie akcji/komendy OPC,
14. uruchomienie zewnętrznego programu/skryptu,
15. wysterowanie wyjścia alarmowego we wskazanym urządzeniu,
16. podświetlenie/zmiana stanu określonego obiektu na mapie synoptycznej,
17. wysłanie zapytania/komendy HTTP,
18. wysłanie pułapki SNMP,
19. wysłanie SMS’a,
20. wywołanie akcji na urządzeniu OPC,
21. zapis do logów systemowych MS Windows,
22. zmiana wartości liczników,
23. włączanie/ wyłączanie urządzenia,
24. wysłanie zdarzenia globalnego.

**System powinien zapewniać integrację z poniższymi rodzajami systemów i urządzeń:**

1. system sygnalizacji włamania i napadu (SSWiN),
2. system kontroli dostępu (SDK),
3. system sygnalizacji pożaru (SSP),
4. moduły wejść/ wyjść,
5. domofony IP,
6. głośniki IP,
7. modemy GSM,
8. urządzenia typu IoT,
9. sieciowe analizatory zapewniające analizę strumieni wideo o wysokiej skuteczności opartej na algorytmach typu DeepLearning.
10. **Aplikacja kliencka**

Oprogramowanie dedykowane dla operatorów systemu wideo powinno spełniać następujące warunki:

1. aplikacja musi być nielicencjonowana, dostępna bez konieczności zakupu/aktywacji licencji komercyjnej,
2. możliwość jednoczesnego połączenia się w wieloma serwerami, grupowanie ich, ilość połączeń nieograniczona,
3. obsługa pracy wielomonitorowej bez ograniczeń programowych w zakresie ilości monitorów,
4. konfigurowalny interfejs użytkownika w zakresie widoków wideo w trybach LIVE oraz odtwarzania,
5. eksportowanie pojedynczych zdjęć oraz fragmentów wideo z archiwum,
6. eksport oraz import pliku konfiguracyjnego dla aplikacji klienckiej,
7. posiadać miniatury obrazu na osi czasu,
8. posiadać miniatury obrazu z kolorem ramki symbolizującym istotność znacznika,
9. posiadać eksportu zdjęć jako dokumentu PDF z opisem operatora i metadanymi przypinanymi do kanałów,
10. możliwość eksportu danych z modułów zewnętrznych i raportów do formatu PDF, XLS, CVS,
11. Możliwość ustawienia formatu do eksportu alarmów z panelu alarmowego: XLS, PDF lub CSV,
12. Możliwość filtrowania wyświetlanych alarmów według parametrów: tekst, priorytet, kanał i grupa,
13. Możliwość wyświetlenia dodatkowych zakładek w panelu alarmowym z innymi parametrami filtracji,
14. Wyszukiwanie nagrań po zdarzeniach VCA według ‘wartości’ w kryteriach wyszukiwania.

Oprogramowanie klienckie powinno zapewniać funkcjonalność w następującym zakresie:

**Podgląd LIVE (na żywo)**

1. strumieniowanie obrazu LIVE do wielu aplikacji klienckich bez wprowadzania opóźnień,
2. obsługa 2-strumieniowości z automatycznym przełączaniem strumieni dla zapewnienia optymalizacji zużycia zasobów sieciowych oraz jednostki klienckiej,
3. obsługa dwukierunkowej transmisji audio w powiązaniu z wybranym kanałem wideo,
4. możliwość globalnej oraz indywidualnej konfiguracji współczynnika proporcji obrazu wideo,
5. możliwość tworzenia tzw. skrótów ułatwiających operatorowi szybkie przełączenie podglądu na kamerę powiązaną ze skrótem w postaci np. strefy półprzezroczystej nałożonej na obraz wideo,
6. możliwość włączenia/wyłączenia przesyłania danych w tle,
7. możliwość powrotu do poprzednio oglądanych podziałów widoku,
8. Możliwość wyboru trybu pracy dla drugiego – auto/ wymuś drugi strumień/ wymuś pierwszy strumień.

**Odtwarzanie natychmiastowe**

1. możliwość natychmiastowego odtworzenia nagrań z wybranego kanału lub wielu kanałów,
2. odtwarzanie z jednoczesnym podglądem obrazu LIVE w sąsiednich oknach.

**Odtwarzanie archiwum**

1. jednoczesne odtwarzanie wielu kanałów z automatyczną obsługą dwustrumieniowości,
2. widok w trybie odtwarzania przechwycony z trybu LIVE,
3. odtwarzanie wprzód oraz wstecz w trybach przyspieszonych z maksymalnym przyspieszeniem 128-krotnym,
4. oś czasu wskazująca obecność danych wideo, audio oraz detekcji ruchu,
5. znaczniki na osi czasu nanoszone automatycznie lub ręcznie przez operatora,
6. możliwość powrotu do poprzednio oglądanych podziałów widoku,
7. możliwość zdefiniowania automatycznego przełączania pomiędzy strumieniami wideo.

**Wyszukiwarka sekwencyjna**

1. podział przeglądanego zakresu materiału wideo z jednej kamery na fragmenty czasowe i szybkie wizualne przeglądanie tego materiału odtwarzanego w wielu oknach z przesunięciem czasowym względem siebie,
2. możliwość powrotu do poprzednio oglądanych podziałów widoku.

**Wyszukiwarka inteligentna Smart-Search**

1. natychmiastowe wyszukanie interesujących nagrań na podstawie uprzedniego wytyczenia regionu zainteresowania, w którym wystąpił ruch (np. zaznaczenie miejsca parkingowego i natychmiastowe wyszukanie nagrań zawierających moment zaparkowania lub wyjazdu pojazdu).

**Obsługa konsoli telemetrycznej**

Z uwagi na ergonomię obsługi i sterowania kamerami obrotowymi PTZ, aplikacja kliencka powinna być kompatybilna z konsolą telemetryczną typu USB wyposażoną w joystick w następującym zakresie:

1. Domyślny zestaw komend sterujących i funkcyjnych,
2. Konfigurowalne komendy mapujące dla dowolnego typu konsoli/joysticka,
3. Obsługa urządzeń sterujących typu Generic DirectShow,
4. Możliwość sterowania wielu okien aplikacji klienckiej za pomocą konsoli telemetrycznej z joystickiem.

**Tryby działania aplikacji**

Aby zapewnić bezpieczeństwo i stabilność pracy stacji klienckiej blokując jednocześnie dostęp do zasobów systemowych, aplikacja musi umożliwiać następujące tryby pracy:

1. Wyłączność: aplikacja kliencka nie pozwala na uruchomienie jakiegokolwiek innego oprogramowania, odblokowanie trybu powinno być możliwe jedynie poprzez wprowadzenie odpowiedniego hasła zabezpieczającego
2. Zawsze na wierzchu: aplikacja kliencka pracuje zawsze jako nadrzędna nie pozwalając innym programom na otwarcie swego interfejsu,
3. Zablokowana: użytkowanie aplikacji jest zablokowane, interfejs użytkownika nie pozwala na wykonanie żadnej operacji. Odblokowanie następuje po wprowadzeniu odpowiedniego hasła,
4. Powinno być możliwe wprowadzenie i zapamiętanie indywidualnych ustawień dla każdego trybu pracy,
5. Aplikacja powinna posiadać tryb natychmiastowego auto-startu w przypadku ponownego uruchomienia stacji klienckiej,
6. Aplikacja powinna pracować nadrzędnie względem wygaszacza ekranu MS Windows.

**Szablony podziału ekranu**

Widoki z podziałami ekranu powinny spełniać następujące funkcjonalności:

1. oferować wbudowany zestaw szablonów domyślnych z różnymi podziałami ekranów
2. szablony definiowane przez użytkownika powinny umożliwiać zapisanie lokalnie na jednostce klienckiej lub globalnie na serwerze centralnym z możliwością współdzielenia dla grupy użytkowników
3. szablony zapisane globalnie powinny być przypisane dla danego użytkownika lub grupy użytkowników i powinny być dostępne niezależnie od stacji klienckiej, na której zaloguje się dany użytkownik
4. pozycje preset (dla kamer PTZ) oraz DPTZ (dla kamer fisheye) powinny być przypisane do danego szablonu i powinny uruchomić się automatycznie po otwarciu danego szablonu
5. sekwencje szablonów powinny umożliwiać automatyczne przełączanie uprzednio zaprogramowanej kolejki widoków zgodnie z ustawionym czasowym interwałem przełączania indywidualnie dla każdego widoku

**Sterowanie PTZ**

Obsługa i sterowanie kamer obrotowych PTZ powinno spełniać następujący zakres:

1. ogólne sterowanie: pan (horyzontalnie), tilt (wertykalnie), zoom (zbliżenie),
2. sterowanie PTZ powinno być dostępne z poziomu aplikacji klienckiej, mobilnej oraz przeglądarki internetowej
3. możliwość ukrycia wirtualnych przycisków sterujących PTZ,
4. wyzwalanie pozycji preset ręcznie (np. za pomocą wirtualnych przycisków) oraz automatycznie (np. po wystąpieniu określonego zdarzenia w systemie),
5. pozycje preset mogą być przypisane jako domyślne pozycje kamer dla danego szablonu/widoku ekranu
6. możliwość definiowania tras patrolowania złożonych z sekwencji presetów.

**Cyfrowy PTZ**

1. funkcja cyfrowego PTZ powinna być dostępna dla dowolnego strumienia wideo,
2. funkcja cyfrowego PTZ powinna być dostępna zarówno dla trybu LIVE (na żywo) jak i odtwarzania archiwum,
3. system powinien zapewniać możliwość przypisania ustawień cyfrowego PTZ do danego szablonu/widoku ekranu jako pozycji domyślnych,
4. system powinien umożliwiać wielokrotne wyświetlenie jednego strumienia wideo z różnymi obszarami zainteresowania, czyli różnymi pozycjami cyfrowego PTZ.

**Rekonstrukcja/prostowanie obrazu z kamery Fisheye (tzw. dewarping)**

1. funkcja prostowania obrazu powinna być dostępna dla dowolnego obrazu dookólnego typu rybie oko,
2. funkcja prostowania obrazu powinna zapewniać tryby: wybrany region, półsfera 180 stopni, panorama 360 stopni,
3. system powinien wspierać prostowanie obrazu dla obiektywów panomorficznych ImmerVision,
4. system powinien wspierać sprzętowo dewarping.

**Obsługa e-map synoptycznych powinna zapewniać:**

1. wyświetlenie mapy w dowolnym oknie ekranu, podobnie jak obrazy wideo,
2. kontekst mapy powinien być interaktywny, tzn. kliknięcie na wybrany marker na mapie powinno powodować wyświetlenie powiązanego kontekstu, np. innej mapy, kanału wideo,
3. Dodawanie wirtualnych przycisków użytkownika na mapie, kliknięcie na przycisk powinno wywołać przypisaną akcję,
4. miniatury obrazu na żywo przy podświetleniu kamery na mapach.

**Eksportowanie materiału wideo (backup)**

1. aplikacja kliencka musi umożliwiać eksportowanie pojedynczych zdjęć oraz fragmentu materiału wideo z/bez audio z wybranego kanału,
2. wielokanałowy eksport materiału wideo musi umożliwiać tworzenie materiału jednorodnego lub w odrębnych plikach dla każdego kanału i posiadać możliwość definiowania rozdzielczości dla eksportu wielokanałowego,
3. eksportowany materiał powinien mieć możliwość wyboru formatu AVI, MP4, MKV,
4. system powinien umożliwiać tzw. anonimizację eksportowanego materiału wideo polegającą na trwałym automatycznym zamaskowaniu twarzy osób lub całych postaci znajdujących się na eksportowanym materiale,
5. wyeksportowany materiał powinien być spakowany archiwizatorem ZIP z zabezpieczeniem hasłem. Archiwum powinno być zaszyfrowane metodą nie gorszą niż AES-256.

**Walidacja znaku wodnego**

1. System powinien znakować i podpisywać wszystkie zapisywane dane wideo,
2. System powinien wspierać i obsługiwać kodeki AVI oraz JPEG,
3. System powinien oferować przenośne narzędzie/odtwarzacz wraz z walidatorem znaku wodnego w eksportowanym materiale.

**Biblioteka**

1. Aplikacja kliencka powinna umożliwiać definiowanie lokalizacji/folderu dla biblioteki, w której zapisywane i przechowywane są eksportowane zdjęcia oraz materiały wideo,
2. Biblioteka daje możliwość drukowania plików graficznych i PDF,
3. materiały znajdujące się w bibliotece powinny być dostępne do skopiowania na wybrany nośnik, do folderu lokalnego lub zasobu sieciowego,
4. użytkownik zgodnie z uprawnieniami powinien mieć możliwość ręcznego usunięcia materiałów znajdujących się w bibliotece.

**Alerty**

Aplikacja kliencka powinna informować użytkownika o błędach połączenia oraz akcjach wykonywanych przez użytkownika

1. **Video Wall (ściana wizyjna złożona z monitorów)**

System powinien zapewniać wygodne zarządzanie tzw. ścianą wizyjną zbudowaną z wielu monitorów, stosowaną w centrum operacyjnym. Funkcjonalność ściany wizyjnej powinna spełniać następujące kryteria:

1. nielimitowana programowo ilość ścian wizyjnych w systemie,
2. funkcja nielicencjonowana, niewymagająca aktywacji dodatkowych licencji komercyjnych,
3. możliwość podłączenia do 100 fizycznych monitorów w obrębie jednej ściany wizyjnej *video-wall,*
4. możliwość wyświetlenia do 100 okien wideo na jednym fizycznym monitorze (w jednym widoku/szablonie),
5. obsługa wyświetlania segmentowego umożliwiającego rozłożenie jednego obrazu na wiele monitorów (np. jeden obraz 4K wyświetlony segmentowo na 4 monitorach FULL HD),
6. przełączanie widoków na ścianie wizyjnej ręcznie z poziomu aplikacji klienckiej,
7. przełączanie widoków na ścianie wizyjnej automatycznie za pomocą makr (scenariuszy) utworzonych w systemie,
8. przełączanie widoków na ścianie wizyjnej w trybie pół-automatycznym za pomocą wirtualnych przycisków użytkownika.
9. **Aplikacja Mobilna**

System musi zapewniać zdalny dostęp do swoich zasobów za pomocą aplikacji mobilnej z zachowaniem gwarancji bezpieczeństwa zdalnego połączenia oraz zapewnieniem funkcjonalności w następującym zakresie:

1. połączenie pomiędzy aplikacją mobilną i serwerem musi być szyfrowane z użyciem SSL, minimum AES-256bit.
2. do wymiany klucza SSL musi być zastosowana metoda nie gorsza niż RSA 2048bit.
3. kompatybilność z systemami iOS oraz Android,
4. odtwarzanie nagrań z wybranego kanału, zgodnie z uprawnieniami użytkownika,
5. wyszukiwanie nagrań według daty i czasu,
6. obsługa kodeków JPEG / H.264 / H.265 / VP8,
7. wyświetlanie obrazu o rozdzielczości 4K,
8. dekodowanie obrazu w trybie sprzętowym lub sprzętowym i programowym (do wyboru),
9. obsługa nagrywania EDGE w pamięci telefonu z uzupełnieniem nagrań w głównej bazie danych po odzyskaniu połączenia smartfonu z serwerem,
10. odbieranie powiadomień alarmowych z systemu w trybie PUSH,
11. bieżące wysyłanie danych lokalizacyjnych GPS z aplikacji mobilnej do systemu,
12. transmisja obrazu z kamery smartfonu do systemu. W systemie powinna być możliwość dodania smartfonu jako kanału wideo, bez zużywania licencji serwerowej,
13. możliwość podziału ekranu w trybach 1x1, 2x1, 2x2, 3x2,
14. przycisk napadowy (jako widget na ekranie startowym) wyzwalający uruchomienie transmisji danych (wideo, GPS, audio) ze smartfonu do systemu,
15. praca sieciowa zarówno w trybie sieci komórkowej jak i w trybie WiFi z obsługą VPN,
16. obsługa kamer PTZ w zakresie sterowania ręcznego, wyzwalania presetów oraz tras,
17. synchronizacja czasu z czasem lokalnym serwera systemowego,
18. obsługa przycisków użytkownika zdefiniowanych w systemie,
19. wyświetlanie bieżących parametrów obrazu live (kodek, bitrate, ilość klatek/sek., rozdzielczość),
20. wsparcie zarządzania użytkownikami Active Directory / LDAP.
21. **Zdalny dostęp za pomocą przeglądarki**

System musi zapewniać zdalny dostęp do swoich zasobów za pomocą przeglądarki internetowej z zachowaniem gwarancji bezpieczeństwa zdalnego połączenia oraz zapewnieniem funkcjonalności w następującym zakresie:

1. połączenie pomiędzy aplikacją mobilną i serwerem musi być szyfrowane z użyciem SSL, minimum 256-128bit,
2. do wymiany klucza SSL musi być zastosowana metoda nie gorsza niż RSA 2048bit,
3. kompatybilność z przeglądarkami Chrome, Firefox (obsługa HTML5 niewymagająca instalacji wtyczek),
4. odtwarzanie nagrań z wybranego kanału, zgodnie z uprawnieniami użytkownika,
5. obsługa dwukierunkowej transmisji audio włącznie z odbiorem audio z aplikacji klienckiej,
6. wsparcie zarządzania użytkownikami Active Directory / LDAP,
7. obsługa kamer PTZ w zakresie sterowania ręcznego oraz wyzwalania presetów,
8. obsługa zarówno strumieni głównych i pomocniczych.