CathexisVision 2020 skrócona specyfikacja A&E

Spis treści

1 Wprowadzenie

Niniejszy dokument stanowi skrócony zarys ogólnych wymagań dotyczących oprogramowania do zarządzania materiałem wizyjnym CathexisVision (które może być dalej określane jako "VMS") i/lub urządzeń peryferyjnych produkowanych przez Cathexis Technologies i dostarczanych przez dystrybutorów Cathexis w wybranych regionach.[1] Pełna specyfikacja znajduje się w kompletnej wersji Specyfikacji A&E CathexisVision.

Wszelkie pytania prosimy kierować na adres support@cat.co.za.

[1] Chociaż firma Cathexis dołożyła wszelkich starań, aby zapewnić dokładność tego dokumentu, nie ma żadnej gwarancji dokładności, ani wyraźnej, ani dorozumianej. Dane techniczne mogą ulec zmianie bez powiadomienia.

2 Architektura systemu

2.1 Architektura systemu

2.1.1 System rejestracji i zarządzania sygnałem wizyjnym jest zarządzany przez oprogramowanie do zarządzania sygnałem wizyjnym (VMS), ma charakter klient-serwer i składa się z następujących elementów:

2.2 Serwery nagrywające

2.2.1 Serwery zapisu powinny zarządzać następującymi funkcjami:

2.2.1.1 Zarządzanie kamerami IP, sieciowymi urządzeniami wejścia/wyjścia oraz koderami wideo.

2.2.1.2 Zapisem obrazu wideo do wybranych pamięci masowych i baz danych, lokalnych lub sieciowych.

2.2.1.3 Zarządzanie dystrybucją bieżącego obrazu wideo do serwerów klienckich, klientów mobilnych oraz ścian wideo.

2.2.1.4 Ułatwianie wyszukiwania i przeglądania nagranego materiału wideo.

2.2.1.5 Zarządzanie zdefiniowanymi przez użytkownika lub technicznymi zdarzeniami, alarmami, ich wyzwalaniem i działaniami.

2.2.1.6 Analityka wideo na wybranych kamerach.

2.2.1.7 Konfiguracja i zarządzanie ANPR oraz integracją z innymi systemami.

2.2.1.8 Zarządzanie prawami dostępu użytkowników.

2.2.2 System powinien umożliwiać łączenie wielu serwerów zapisu w celu utworzenia obiektu. Serwery te mogą być zlokalizowane geograficznie w jednym lub wielu fizycznych miejscach.

2.2.3 Nie jest wymagany "serwer zarządzający". Jeden z serwerów rejestrujących jest automatycznie wyznaczany jako serwer "zarządzający" lub "główny" dla tej funkcji.

2.2.4 Nie jest wymagany serwer analizy wideo. Funkcja ta powinna być realizowana przez serwery nagrywające.

2.2.5 Oprogramowanie serwera nagrywającego powinno obsługiwać systemy operacyjne Windows i Linux.

2.3 Serwery klienckie

2.3.1 Oprogramowanie serwera klienckiego powinno obsługiwać zarówno systemy operacyjne Windows jak i Linux.

2.3.2 Oprogramowanie serwera klienckiego powinno umożliwiać następujące czynności:

2.3.2.1 Wykonywanie wszystkich funkcji związanych z ustawieniem i konfiguracją obiektu, który może zawierać wiele serwerów rejestrujących.

2.3.2.2 Wyświetlanie i przeglądanie wszystkich kamer w obiekcie.

2.3.2.3 Podłączenie do bramy zarządzania alarmami w celu przeglądania alarmów i zarządzania pojedynczą lub wieloma lokalizacjami.

2.3.2.4 Sterowanie funkcjami ściany wizyjnej za pomocą panelu synoptycznego.

2.3.2.5 Konfigurowanie map lokalizacji i zarządzanie nimi.

2.3.2.6 Przeglądanie i zarządzanie bazami danych ANPR i innymi bazami integracyjnymi.

2.3.2.7 Przeglądanie meta baz danych i zarządzanie nimi.

2.4 Serwery ściany wizyjnej

2.4.1 Serwery ściany wizyjnej powinny zawierać oprogramowanie ściany wizyjnej w celu:

2.4.1.1 Obsługę wielu serwerów, z których każdy jest w stanie pomieścić wiele monitorów, których ilość będzie zależna od sprzętu.

2.4.1.2 Wyświetlanie do 64 obrazów z kamer na każdym monitorze na polecenie systemu VMS.

2.4.1.3 Wyświetlanie do 64 strumieni wideo na każdy monitor w zależności od instrukcji z systemu VMS.

2.4.1.4 Wykonywanie obchodów kamer i obchodów układów (salwa).

2.4.1.5 Sterowanie za pomocą panelu synoptycznego w oprogramowaniu klienckim VMS.

2.5 Serwer awaryjny

2.5.1 Serwery awaryjne powinny przejąć wszystkie funkcje serwerów zapisu w przypadku awarii lub wyłączenia serwera zapisu.

2.5.2 Serwery awaryjne ułatwiają także odtwarzanie w przypadku awarii poprzez automatyczne przywrócenie zastąpionego lub naprawionego serwera.

2.5.3 Przełączenie awaryjne ma charakter "hotspare".

2.5.4 W jednej lokalizacji można zainstalować wiele serwerów awaryjnych.

2.5.5 Czas oczekiwania na przełączenie awaryjne powinien być konfigurowalny i nie powinien przekraczać 30 sekund.

2.6 Brama zarządzania alarmami

2.6.1 Oprogramowanie Alarm Management Gateway powinno obsługiwać zarówno systemy operacyjne Windows, jak i Linux.

2.6.2 Oprogramowanie Alarm Management Gateway powinno odbierać alarmy z wielu lokalizacji z wieloma serwerami i posiadać konfigurowalne procedury ich obsługi.

2.6.3 Bramka alarmowa powinna realizować routing i zarządzanie połączeniami dla automatycznego łączenia i przesyłania strumieniowego obrazu z lokalizacji, którego szczegółowość powinna być określona przez konkretny odebrany alarm.

2.7 Pamięć masowa i bazy danych

2.7.1 System powinien umożliwiać podział baz danych na wiele dysków i/lub sieciowych urządzeń pamięci masowej.

2.7.2 Obsługiwane powinny być najpopularniejsze protokoły pamięci masowej, w tym SATA, SAS, SSD, DAS, SAN, NAS oraz iSCSI.

2.7.3 System powinien udostępniać własny system baz danych do przechowywania materiałów wideo, a nie opierać się na bazach danych innych firm (np. MySQL) w tej funkcji.

2.7.4 System powinien umożliwiać tworzenie dedykowanych baz danych, w tym:

2.7.4.1 Ogólna baza danych wideo.

2.7.4.2 Baza metadanych (integracji).

2.7.4.3 Baza zdarzeń systemowych.

2.7.4.4 Baza integracji ANPR.

2.7.4.5 Baza danych klasyfikacji obiektów.

2.7.5 Wszystkie bazy danych powinny umożliwiać następujące czynności:

2.7.5.1 Odtwarzanie obrazu wideo ze zintegrowanego odtwarzacza wideo.

2.7.5.2 Filtrowanie i przeszukiwanie wpisów w bazach danych.

2.7.5.3 Wyświetlanie nakładek i/lub metadanych związanych z nagraniem.

2.7.5.4 Eksportowanie wpisów do bazy danych w formacie PDF lub CSV.

2.7.5.5 Archiwizacja nagrań wideo i powiązanych z nimi metadanych za pomocą zintegrowanego odtwarzacza wideo.

2.7.5.6 Postarzanie wideo. Materiał wideo z jednej bazy danych może być transkodowany do zmniejszonego rozmiaru i przechowywany przez dłuższy czas w drugiej bazie danych.

2.7.5.7 Niszczenie bazy danych, które trwale niszczy materiał wideo starszy niż maksymalny limit dni zapisu.

2.8 Synchronizacja czasu

2.8.1 Wszystkie systemy powinny być zdolne do synchronizacji czasu przy użyciu protokołu NTP (Network Time Protocol).

2.9 Cyberbezpieczeństwo

2.9.1 System powinien zapewniać bezpieczną komunikację pomiędzy komponentami systemu VMS, w tym:

2.9.1.1 Serwery nagrywające do klientów.

2.9.1.2 Serwery nagrywające do innych serwerów nagrywających.

2.9.1.3 Serwery nagrywające do Ścian Wizyjnych.

2.9.1.4 Serwery zapisu do bramy zarządzania alarmami.

2.9.2 Podczas komunikacji pomiędzy komponentami systemu VMS stosowane są następujące środki bezpieczeństwa:

2.9.2.1 Silnik szyfrujący powinien używać szyfrów openssl (SHA512 hashes, ephemeral DH-RSA with forward secrecy [DH 2048 bit] oraz AES-GCM 128-bit symmetric ciphers) równoważnych TLS 1.3.

2.9.2.2 Hasła nigdy nie są przechowywane jako zwykły tekst, lecz są hashtagowane za pomocą SHA512.

2.9.2.3 Dane uwierzytelniające do logowania są negocjowane przy użyciu RSA1024.

2.9.2.4 Wrażliwe kanały komunikacyjne są szyfrowane przy użyciu AES128/CBC.

2.9.2.5 Do weryfikacji integralności wykorzystywany jest HMAC.

2.9.2.6 Wszystkie połączenia ze stronami zewnętrznymi obsługują różne poziomy szyfrowania:

2.9.2.6.1 Wyłączone.

2.9.2.6.2 Minimalny - szyfrowane są tylko połączenia krytyczne.

2.9.2.6.3 Secure (domyślnie) - szyfrowane są wszystkie połączenia z wyjątkiem tych, w których występuje duża ilość wideo.

2.9.2.6.4 All - wszystkie połączenia, w tym połączenia wideo o dużej objętości, powinny być szyfrowane.

2.9.2.7 Infrastruktura klucza publicznego (PKI) jest zarządzana wewnętrznie przez VMS w celu zwiększenia bezpieczeństwa.

2.9.3 System powinien zapewniać bezpieczeństwo i integralność zapisanego obrazu za pomocą następujących środków:

2.9.3.1 Podwójne klucze RSA1024 (do podpisywania) są używane w celu zabezpieczenia integralności eksportowanego/archiwizowanego materiału wideo.

2.9.3.2 Opcjonalne szyfrowanie wykorzystuje szyfrowanie blokowe AES128 z losowym IV na blok i hasłem wygenerowanym przez użytkownika.

2.9.3.3 Zarchiwizowane wideo może zawierać znacznik autoryzacji w celu wskazania źródła informacji (np. informacji o użytkowniku).

2.9.3.4 Ograniczenie odtwarzania zarchiwizowanych materiałów wideo i metadanych do odtwarzania za pomocą własnego odtwarzacza wideo systemu VMS.

2.9.3.5 Eksportowane/zarchiwizowane materiały wideo mogą być ograniczone do odtwarzania sterowanego hasłem.

2.9.4 System powinien, w zakresie, w jakim te środki są wspierane przez producentów, zapewnić bezpieczeństwo podłączonych kamer IP za pomocą następujących środków:

2.9.4.1 Bezpieczne połączenie kamer:

2.9.4.1.1 HTTP: protokół HTTP.

2.9.4.1.2 Szyfrowane połączenia sterujące HTTPS.

2.9.4.1.3 Szyfrowane połączenia SSL/TLS.

2.9.4.1.4 Obsługa przez CURL (client-side URL transfer library).

2.9.4.2 Bezpieczne sterowanie kamerą:

2.9.4.2.1 RTSP - protokół strumieniowania w czasie rzeczywistym.

2.9.4.2.2 Sterowanie szyfrowane HTTPS.

2.9.4.3 Bezpieczna transmisja strumienia wideo:

2.9.4.3.1 RTP - sterowanie transportem w czasie rzeczywistym.

2.9.4.3.2 Zaszyfrowane wideo.

3 Wymagania dotyczące oprogramowania do zarządzania sygnałem wizyjnym (VMS)

3.1 Obsługa kamer IP

3.1.1 System VMS powinien obsługiwać zarówno interfejs Onvif-S, jak i natywny interfejs kamery.
3.1.2 System VMS powinien obsługiwać kamery sieciowe z wieloma głowicami.
3.1.3 Maszyny wirtualne powinny obsługiwać nadajniki sygnału wizyjnego.
3.1.4 System VMS powinien obsługiwać protokoły kamer MJPEG, H.264, H.265 i MxPEG.
3.1.5 Interfejs VMS do kamery powinien być zgodny z UPnP (universal plug and play), jeśli kamera obsługuje tę funkcję.
3.1.6 System VMS powinien obsługiwać strumienie wideo o zmiennej i stałej przepływności.
3.1.7 VMS powinien obsługiwać wiele strumieni i rozdzielczości wideo, ograniczonych jedynie przez same zintegrowane kamery.
3.1.8 VMS powinien obsługiwać kamery 360 i 180 stopni oraz posiadać wbudowane oprogramowanie, które umożliwia korekcję zniekształceń takich kamer.
3.1.9 VMS powinien obsługiwać kamery obrotowe:

3.1.9.1 VMS powinien mieć możliwość zaprogramowania pozycji Preset kamer PTZ oraz przypisania unikalnych nazw do każdej pozycji Preset.
3.1.9.2 VMS powinien obsługiwać funkcje area-zoom w wybranych kamerach, umożliwiając obracanie i przybliżanie kamery do obszaru wybranego przez użytkownika.
3.1.9.3 Priorytet sterowania PTZ powinien być przydzielany na zasadzie hierarchii, zgodnie z hierarchią poziomów praw dostępu.

3.1.10 System VMS powinien oferować tylko te ustawienia kamery, które są dostępne dla konkretnej kamery.
3.1.11 VMS powinien obsługiwać wejścia i wyjścia z kamer.
3.1.12 VMS powinien obsługiwać zsynchronizowany dźwięk z kamery.
3.1.13 VMS musi obsługiwać dwukierunkowy sygnał audio.
3.1.14 System VMS powinien mieć możliwość odbierania zdarzeń analitycznych z wybranych kamer, które oferują taką możliwość.
3.1.15 VMS powinien umożliwiać użytkownikowi "nawigację" bezpośrednio do adresu URL kamery lub strony internetowej z okna konfiguracji kamery.
3.1.16 Kamera powinna mieć możliwość skonfigurowania jako kamera "ukryta".
3.1.17 System VMS powinien obsługiwać strefy prywatności, które umożliwiają użytkownikowi zdefiniowanie obszarów, które mają być maskowane z widoku operatora.

3.2 Graficzny interfejs użytkownika

3.2.1 System VMS powinien obsługiwać tłumaczenie graficznego interfejsu użytkownika (GUI) na wiele języków, w tym:

3.2.1.1 Arabski.
3.2.1.2 Holenderski.
3.2.1.3 Angielski.
3.2.1.4 Francuski.
3.2.1.5 Węgierski.
3.2.1.6 Włoski.
3.2.1.7 Portugalski.
3.2.1.8 Hiszpański.

3.2.2 System VMS powinien umożliwiać zapis obrazu z kamer do baz danych zdefiniowanych przez użytkownika.
3.2.3 System VMS powinien zapewniać konfigurowalne opcje zapisu przed i po zdarzeniu.
3.2.4 System VMS powinien zapewniać rzeczywiste środowisko "triplex", umożliwiając nagrywanie, podgląd na żywo i odtwarzanie na wielu kamerach jednocześnie.
3.2.5 System VMS powinien umożliwiać użytkownikom definiowanie wielu baz danych oraz wybór bazy, do której mają być zapisywane nagrania z poszczególnych kamer.
3.2.6 System VMS powinien obsługiwać zapis obrazu i dźwięku.
3.2.7 System VMS powinien umożliwiać inicjowanie zapisu za pomocą jednej z następujących metod:

3.2.7.1 Ciągła.
3.2.7.2 Harmonogram czasowy.
3.2.7.3 Po wystąpieniu zdarzenia.
3.2.7.4 Inicjacja przez użytkownika.

3.2.8 Użytkownicy powinni mieć możliwość wyboru który strumień wideo z wybranych kamer ma być rejestrowany.
3.2.9 System VMS powinien umożliwiać zapis z jednej kamery do wielu baz danych jednocześnie.
3.2.10 System VMS powinien umożliwiać użytkownikowi podgląd od 1 do 64 kamer na ekranie w zdefiniowanych przez użytkownika układach.
3.2.11 System VMS powinien zapewniać możliwość przeglądania układów na monitorach ściany wizyjnej.
3.2.12 System VMS powinien udostępniać panel synoptyczny do sterowania wieloma monitorami na ścianie wizyjnej.
3.2.13 System powinien udostępniać funkcję mapowania sąsiednich kamer, która umożliwia łączenie w oprogramowaniu geograficznie bliskich kamer oraz łatwą nawigację między połączonymi kamerami w interfejsie operatora w celu śledzenia obiektów/podejrzanych poruszających się w obrębie wielu kamer.
3.2.14 Śledzenie podejrzanego ma na celu dołączenie funkcji sąsiadującego mapowania kamer do pożądanego zastosowania w dziedzinie bezpieczeństwa.
3.2.15 VMS powinien umożliwiać użytkownikom tworzenie układów ekranu i zapisywanie ich pod nazwami zdefiniowanymi przez użytkownika.
3.2.16 Układy zdefiniowane przez użytkownika powinny być wyświetlane jako ikony w panelu zasobów i łatwo przywoływane przez użytkownika.
3.2.17 VMS powinien umożliwiać użytkownikom cyfrowe powiększanie obrazu z kamery za pomocą kółka przewijania myszy.
3.2.18 System VMS powinien umożliwiać wykonywanie obchodów kamer (sekwencji) w panelu kamery lub na wybranym monitorze z konfigurowalnymi opóźnieniami czasowymi pomiędzy poszczególnymi sekwencjami kamer. Powinno się to odbywać poprzez nakładanie strzałek wskazujących kierunek na następną, najbliższą kamerę.
3.2.19 System powinien umożliwiać użytkownikowi tworzenie zakładek ulubionych układów kamer w trybie podglądu na żywo tylko dla zasobów, do których użytkownik ma prawa dostępu.
3.2.20 System powinien zapewniać system zarządzania obrazami referencyjnymi, który tworzy obrazy referencyjne z oznaczeniem czasu orientacji wszystkich kamer serwera.

3.2.20.1 System powinien umożliwiać porównanie przechwyconych obrazów referencyjnych z bieżącym (nieprzechwyconym) obrazem serwera.

3.2.20.2 System powinien wyświetlać procentową różnicę pomiędzy dwoma porównywanymi obrazami.

3.2.21 Jeśli w kamerze skonfigurowano wiele strumieni wideo do podglądu na żywo, użytkownik powinien mieć możliwość wyboru strumienia wideo, który ma być wyświetlany. Umożliwia to użytkownikom wyświetlanie obrazów o niższej rozdzielczości na potrzeby monitoringu poza siedzibą firmy.

3.2.22 System VMS powinien być wyposażony w wielowarstwowy system zarządzania prawami dostępu.

3.2.23 System VMS powinien umożliwiać administratorowi przypisanie cech i funkcji do wybranych poziomów użytkowników.

3.2.24 VMS powinien obsługiwać LDAP, OpenLDAP oraz Windows Active directory.

3.2.25 System powinien udostępniać dzienniki audytu z kompletem zapisów wszystkich działań użytkowników.

3.2.26 System powinien umożliwiać administratorom filtrowanie logów audytowych według następujących kryteriów:

3.2.26.1 Godzina.

3.2.26.2 Okres czasu.

3.2.26.3 Identyfikacja użytkownika.

3.2.26.4 Zasoby (np. kamery).

3.2.26.5 Działania użytkownika.

3.2.27 VMS powinien umożliwiać eksport logów audytowych w formacie pliku CSV.

3.2.28 System VMS powinien umożliwiać użytkownikom z prawami dostępu możliwość archiwizacji (eksportu) wybranych materiałów wideo do wybranego folderu lub na zewnętrzny nośnik danych.

3.2.29 W celu zapewnienia bezpieczeństwa materiału wideo, wyeksportowany materiał wideo jest cyfrowo "podpisany" przy użyciu kluczy RSA1024, a opcjonalne szyfrowanie odbywa się przy użyciu szyfrowania blokowego AES128 z losowym IV na blok i hasłem generowanym przez użytkownika.

3.2.30 VMS powinien posiadać następujące funkcje ochrony prywatności zarchiwizowanych (wyeksportowanych) nagrań wideo:

3.2.30.1 Zdefiniowany przez użytkownika znacznik autoryzacji.

3.2.30.2 Hasło zdefiniowane przez użytkownika, które musi być wprowadzone przed odtworzeniem wyeksportowanego obrazu.

3.2.31 System VMS powinien umożliwiać użytkownikowi przeglądanie nagrań z wielu kamer jednocześnie.

3.2.32 System VMS powinien umożliwiać przeglądanie nagrań z pokładowego Edge'a obsługiwanych kamer.

3.2.33 VMS powinien umożliwiać użytkownikowi synchronizację odtwarzania obrazu z wielu kamer.

3.2.34 System VMS powinien zapewniać zaawansowane funkcje wyszukiwania umożliwiające użytkownikom sprawne odnajdywanie odpowiednich materiałów wideo w następujący sposób:

3.2.34.1 Oś czasu:

3.2.34.1.1 VMS powinien umożliwiać użytkownikom nawigację do nagranego materiału filmowego poprzez przeciąganie paska osi czasu.

3.2.34.1.2 VMS powinien umożliwiać użytkownikom nawigację do zarejestrowanego materiału filmowego poprzez wybranie daty i godziny z kalendarza.

3.2.34.1.3 Użytkownik powinien mieć możliwość "powiększania" paska osi czasu za pomocą kółka przewijania myszy.

3.2.34.2 Wyszukiwanie ruchu:

3.2.34.2.1 VMS powinien zawierać funkcję Motion Search, która umożliwia użytkownikowi odnalezienie materiału wideo poprzez wybranie obszaru w obrębie widoku kamery i wykonanie wyszukiwania.

3.2.34.2.2 Funkcja ta powinna wykorzystywać metadane ruchu wideo przechowywane na serwerze w celu przeprowadzenia tego wyszukiwania.

3.2.34.2.3 Każdy ruch wykryty w tym obszarze powinien być wyświetlany na pasku osi czasu w interfejsie użytkownika.

3.2.34.3 Wyszukiwanie migawkowe (Snapshot Search):

3.2.34.3.1 VMS powinien zawierać funkcję Snapshot Search, która umożliwia użytkownikom przeglądanie zrzutów podzielonych na wybrany czas w celu łatwego odnalezienia zaistniałych incydentów.

3.2.34.3.2 Funkcja ta powinna umożliwiać użytkownikom łatwe zmniejszanie zakresu czasowego (drilling-down) poprzez przeciąganie pomiędzy dwoma zrzutami.

3.2.34.3.3 Użytkownik powinien mieć możliwość odtwarzania zarejestrowanego materiału filmowego z wybranego ujęcia bezpośrednio z okna Snap-Search.

3.2.34.4 Nakładka ścieżek aktywności:

3.2.34.4.1 System VMS powinien udostępniać na żądanie nakładkę ruchu wideo z przeszłości.

3.2.34.4.2 Użytkownik powinien mieć możliwość natychmiastowego odtwarzania obrazu wideo z wybranego czasu nakładki za pomocą poleceń myszy.

3.2.34.5 Mapy cieplne:

3.2.34.5.1 System powinien umożliwiać wyświetlanie nakładki mapy cieplnej w celu wskazania obszarów ruchu na obrazie z kamery.

3.2.34.5.2 System powinien umożliwiać dopracowanie wyników mapy cieplnej przy użyciu analizy okresowej.

3.2.35 VMS powinien oferować następujące funkcje zarządzania zdarzeniami:

3.2.35.1 Zdarzenia mogą być wyzwalane przez:

3.2.35.1.1 Wyzwalacze analityki wideo z analityki pokładowej lub analityki Edge (zależne od kamery).

3.2.35.1.2 Wejścia/wyjścia kamery lub inne wejścia/wyjścia.

3.2.35.1.3 Wyzwalacze inicjowane przez użytkownika.

3.2.35.1.4 Wyzwalacze zdarzeń innych producentów (np. kontrola dostępu, centrale sygnalizacji włamania i pożaru).

3.2.35.1.5 Alarmy techniczne:

3.2.35.1.5.1 Sabotaż kamery.
3.2.35.1.5.2 Awaria kamery.
3.2.35.1.5.3 Awaria dysku twardego.
3.2.35.1.5.4 Błędy bazy danych.
3.2.35.1.5.5 Przełączanie systemu w przypadku awarii.
3.2.35.1.5.6 Błędy serwera oprogramowania.
3.2.35.1.5.7 Alarm łączności sieciowej.
3.2.35.1.5.8 Alarmy restartu systemu.
3.2.35.1.5.9 Alarm zaplanowanej archiwizacji.
3.2.35.1.6 Alarm testowy.
3.2.35.2 Działania w ramach zdarzeń obejmują:
3.2.35.2.1 Zapis wybranego przez kamerę strumienia wideo do wybranej bazy danych.
3.2.35.2.2 Przełączanie kamery na wybrany monitor ściany wizyjnej lub monitor lokalny.
3.2.35.2.3 Odtwarzanie wybranego klipu dźwiękowego do:
3.2.35.2.3.1 Wyjścia audio serwera klienta.
3.2.35.2.3.2 Wyjścia audio kamery.
3.2.35.2.4 Wysyłanie alarmu do bramy zarządzania alarmami.
3.2.35.2.5 Wysyłanie alarmu do interfejsu serwera klienckiego.
3.2.35.2.6 Wysyłanie wiadomości e-mail.
3.2.35.2.7 Wysyłanie wiadomości SMS.
3.2.35.2.8 Przesunięcie kamery PTZ na zaprogramowaną pozycję.
3.2.36 VMS powinien obsługiwać zarówno klientów mobilnych IOS, jak i Android.
3.2.37 System VMS powinien umożliwiać wyświetlanie nakładek tekstowych na obrazie wideo z urządzeń innych producentów.
3.2.38 System VMS powinien mieć możliwość integracji z systemami innych firm, takimi jak kontrola dostępu, alarmy włamaniowe i centrale sygnalizacji pożaru w celu zapewnienia następujących funkcji:

3.2.38.1 Odbieranie danych/komunikatów o zdarzeniach z systemów stron trzecich.
3.2.38.2 Kojarzenie jednej lub więcej kamer z określonymi urządzeniami systemów innych firm.
3.2.38.3 Przechowywanie danych z systemów trzecich wraz z powiązanym z nimi obrazem w wybranych bazach danych.
3.2.38.4 Wyświetlanie nakładek z danymi z systemów innych firm w podglądzie na żywo.
3.2.38.5 Umożliwienie przeszukiwania bazy danych integracji systemów firm trzecich w celu łatwego odnajdywania transakcji i powiązanych z nimi materiałów wideo.
3.2.39 System VMS powinien mieć możliwość połączenia z klawiaturami/joystickami producenta lub innych firm.
3.2.40 System VMS powinien udostępniać funkcję hierarchicznej mapy, która umożliwia użytkownikowi:

3.2.40.1 Tworzenie map przy użyciu plików JPG lub PNG.
3.2.40.2 Dodawanie kamer lub innych zasobów z poziomu edytora map.
3.2.40.3 Tworzenie wielokątów, które mogą wyświetlać zdefiniowane przez użytkownika akcje i "wyskakiwać" w przypadku wystąpienia zdarzenia.
3.2.40.4 Tworzenie ikon wyzwalających akcję użytkownika.
3.2.40.5 Tworzenie obszarów PTZ Preset, które po kliknięciu automatycznie przesuwają kamerę PTZ na przypisaną pozycję.

3.2.40.6 Przejście do szczegółów różnych warstw mapy z poziomu interfejsu użytkownika.
3.2.40.7 Automatyczne połączenie ze zdalną witryną z poziomu interfejsu mapy.
3.2.41 VMS powinien zapewniać infrastrukturę umożliwiającą raportowanie monitorowania kondycji oraz stanu systemu:

3.2.41.1 Awarie kamer, logi, status i czas do naprawy.
3.2.41.2 Użytkowanie bazy danych:
3.2.41.2.1 Podział na kamery.
3.2.41.2.2 Stawka według kamery/godziny/kamery na godzinę.
3.2.41.3 Histogram częstotliwości zdarzeń.
3.2.41.4 Zdarzenia na godzinę.
3.2.41.5 Dysk.
3.2.41.6 Zdarzenia.
3.2.41.7 Systemy plików.
3.2.41.8 Sprzęt.
3.2.41.9 Licencje.
3.2.41.10 Zapytania protokołu czasu sieciowego.
3.2.41.11 Ponowne uruchomienia i przyczyny ponownych uruchomień, w tym:
3.2.41.11.1 Restarty serwera oprogramowania.
3.2.41.11.2 Restarty spowodowane awarią zasilania.
3.2.41.11.3 Ponowne uruchomienia użytkowników.
3.2.41.11.4 Ponowne uruchomienie zdalnego użytkownika.
3.2.41.11.5 Czas restartu.
3.2.41.12 Ustawienia i konfiguracja zapisu, czasy (systemu na kamerę) oraz awarie zapisu.
3.2.41.13 Ustawienia i konfiguracja systemu.
3.2.41.14 Awarie serwera oprogramowania.
3.2.41.15 Czas pracy urządzenia.
3.2.41.16 Raporty o aktualnie niedziałających kamerach.
3.2.41.17 Alerty kondycji na pasku stanu. Komunikat będzie wyświetlany, jeśli dysk, na którym jest zainstalowany NVR, zapełni się.

3.3 Przełączanie awaryjne

3.3.1 System powinien obsługiwać przełączanie awaryjne serwerów n:1 i n:n.
3.3.2 Serwer awaryjny jest serwerem rezerwowym (hotspare) i przejmuje funkcje każdego serwera, który uległ awarii, w tym serwera głównego.
3.3.3 Przełączanie awaryjne obejmuje wszystkie funkcje serwera rejestracji.
3.3.4 Przełączenie awaryjne obejmuje wszystkie funkcje zarządzania ścianą wizyjną.
3.3.5 Przełączenie awaryjne obejmuje wszystkie funkcje zarządzania zdarzeniami i działaniami.
3.3.6 W przypadku awarii systemu serwer awaryjny zapisuje materiał wizyjny do dedykowanej bazy danych.
3.3.7 W przypadku wymiany uszkodzonego serwera materiał filmowy z awaryjnej bazy danych jest automatycznie ponownie wprowadzany do pierwotnej bazy danych.

3.4 Klawiatura/sterownik

3.4.1 System powinien być wyposażony w zintegrowaną klawiaturę/sterownik.
3.4.2 System powinien umożliwiać konfigurację czułości PTZ w oprogramowaniu.

3.4.3 Klawiatura powinna umożliwiać szybkie wybieranie za pomocą klawiszy kamer, presetów, monitorów, wyjść, tras kamer (sekwencji) oraz układów ekranów.

3.4.4 Przyciski funkcyjne kamer PTZ powinny być dostępne dla palców ręki obsługującej joystick, tak, aby operatorzy nie musieli rezygnować z kontroli nad joystickiem.

3.4.5 Wyświetlacz LCD klawiatury powinien mieć możliwość zapisu przez system nadzoru cyfrowego.

3.4.6 Diody LED na klawiaturze powinny wskazywać stan klawiszy i funkcji.

3.5 Analityka wideo

3.5.1 System VMS powinien zapewniać wbudowane własne funkcje analizy obrazu wideo dostępne na podstawie licencji w następujący sposób:

3.5.1.1 Podstawowa wizyjna detekcja ruchu.

3.5.1.2 Zaawansowana wizyjna detekcja ruchu z dynamicznym modelowaniem tła i algorytmami uczenia.

3.5.1.3 Ruch w obszarze.

3.5.1.4 Brak ruchu w obszarze, w którym spodziewany jest ruch.

3.5.1.5 Proste rejestrowanie ruchu.

3.5.1.6 Przekraczanie linii obiektu.

3.5.1.7 Kierunek obiektu.

3.5.1.8 Prędkość obiektu.

3.5.1.9 Postój obiektu.

3.5.1.10 Obiekt wjeżdżający na obszar.

3.5.1.11 Obiekt opuszczający obszar.

3.5.1.12 Klasyfikacja obiektów.

3.5.1.12.1 System powinien posiadać możliwość obsługi dedykowanej bazy danych klasyfikacji obiektów w celu przechowywania klasyfikacji obiektów.

3.5.1.13 Wykrywanie pozostawionych obiektów.

3.5.1.14 Sabotaż kamery.

3.5.1.15 Liczenie obiektów.

3.5.2 Interfejs użytkownika systemu VMS powinien udostępniać nakładki analityki wizyjnej pokazujące następujące elementy:

3.5.2.1 Aktywność analityki wideo.

3.5.2.2 Wyzwalacze analityki wizyjnej.

3.5.2.3 Strefy analizy obrazu.

3.5.3 Algorytmy analizy obrazu powinny mieć możliwość inicjowania niepowtarzalnych zdarzeń w oprogramowaniu VMS

3.6 Automatyczne rozpoznawanie tablic rejestracyjnych (ANPR)

3.6.1 System ANPR powinien zapewniać możliwość rozpoznawania tablic rejestracyjnych według regionów oraz posiadać następujące możliwości:

3.6.1.1 Rozwiązanie ANPR powinno działać z dowolnymi odpowiednimi kamerami IP lub odpowiednią rozdzielczością, liczbą klatek na sekundę i szybkością migawki z odpowiednim oświetleniem.

3.6.2 Możliwość konfiguracji, która powinna obejmować:

3.6.2.1 Regulację pochylenia.

3.6.2.2 Regulację obszaru identyfikacji.
3.6.2.3 Regulację oczekiwanej wielkości znaków tablic rejestracyjnych.
3.6.2.4 Test nagrywania materiału filmowego.

3.6.3 Nakładki z informacjami o tablicach rejestracyjnych są wyświetlane na obrazie bieżącym i/lub nagranym i obejmują:

3.6.3.1 Dane dotyczące tablic rejestracyjnych.
3.6.3.2 Zrzut tablic rejestracyjnych.

3.6.4 System powinien umożliwiać grupowanie danych dotyczących tablic rejestracyjnych w określone kategorie zdefiniowane przez użytkownika, takie jak goście, personel, biała lista, czarna lista itd.

3.6.5 System powinien zapewniać możliwość tworzenia reguł zdarzeń/alarmów w przypadku wykrycia tablicy rejestracyjnej z wybranej grupy (na przykład w przypadku wykrycia tablicy rejestracyjnej z grupy pracowników można zażyczyć sobie automatycznego otwarcia szlabanu. W przypadku wykrycia tablicy rejestracyjnej z grupy z czarnej listy można uruchomić alarm).

3.6.6 System powinien umożliwiać import informacji o tablicach rejestracyjnych w celu włączenia ich do wybranych grup (np. personel, czarna lista).

3.6.7 System powinien umożliwiać użytkownikowi dodawanie niestandardowych informacji do znanych tablic rejestracyjnych. Np. typ pojazdu, nazwisko osoby itp.

3.6.8 System powinien umożliwiać filtrowanie bazy danych ANPR według szeregu opcji, w tym między innymi według następujących kryteriów:

3.6.8.1 Godzina/Data.
3.6.8.2 Tablice rejestracyjne/grupy.
3.6.8.3 Zaufanie (dokładność wychwytywania tablic rejestracyjnych w procentach).
3.6.8.4 Detektor ANPR.
3.6.8.5 Kamera.
3.6.8.6 Nazwa kierowcy/firmy.
3.6.8.7 Typ pojazdu/marka/model/kolor.
3.6.8.8 Miejsce wydania (w zależności od regionu).
3.6.8.9 Kolor tła, kolor tekstu i kształt tablicy rejestracyjnej.
3.6.8.10 Umiejscowienie tablicy rejestracyjnej na samochodzie (przód/tył).
3.6.8.11 Położenie pojazdu na pasie ruchu (wjazd/wyjazd).
3.6.8.12 Raporty ANPR w oparciu o filtry.

3.7 Brama zarządzania alarmami

3.7.1 System powinien zapewniać scentralizowany system zarządzania alarmami/zdarzeniami, który umożliwia zarządzanie zdarzeniami i/lub alarmami z lokalizacji lokalnej lub z wielu lokalizacji zdalnych.

3.7.2 System zarządzania alarmami powinien w określonych odstępach czasu monitorować połączenia z jednostkami zdalnymi poprzez funkcję "pulsu witryny" w danej lokalizacji. Generuje on sygnał wyzwalający, gdy zdalna jednostka alarmująca nie wysyła sygnału pulsu.

3.7.3 Interfejs alarmowy powinien mieć kontrolowany dostęp, być niezależny od reszty oprogramowania i powinien posiadać własne narzędzie do zarządzania użytkownikami.

3.7.4 System powinien wyświetlać alarmy w oddzielnych panelach w zależności od stanu:

3.7.4.1 Przychodzący (oczekujący na obsługę przez operatora).

3.7.4.2 Bieżący (obsługiwany przez operatora).

3.7.4.3 Zarchiwizowany (już obsługiwany przez operatora).

3.7.5 System powinien umożliwiać dostosowanie powiadomień dźwiękowych o alarmie przychodzącym do potrzeb użytkownika.

3.7.6 System powinien wyświetlać alarmy w zależności od priorytetu, oznaczonego różnymi kolorami, zgodnie z konfiguracją dla alarmów zdarzeniowych.

3.7.7 System powinien mieć możliwość odtwarzania alarmów dźwiękowych zgodnie z poziomem priorytetu alarmu.

3.7.8 Jeżeli alarmy są obsługiwane przez wielu operatorów, system powinien informować wszystkich operatorów o stanie alarmu oraz o tym, kto obsługuje dany alarm.

3.7.9 System powinien umożliwiać operatorom reagowanie na alarm oraz:

3.7.9.1 Automatycznie połączyć się z miejscem, z którego zainicjowany został alarm.

3.7.9.2 Automatyczne wyświetlanie mapy miejsca, z którego zainicjowany został alarm.

3.7.10 System powinien umożliwiać czasowe wyłączenie (zablokowanie) powtarzających się nieważnych alarmów na określony czas. Blokada ta powinna być określana z poziomu jednostki bramowej i powinna wymagać komentarza ze strony operatora blokującego.

3.7.11 System powinien umożliwiać operatorom jednoczesne usuwanie wielu alarmów z kolejki alarmów przychodzących.

3.7.12 System powinien umożliwiać operatorom dodawanie komentarzy do alarmów bieżących i archiwalnych. Aby ułatwić szybkie reagowanie, komentarze domyślne powinny być wybierane z menu, ale powinna istnieć również możliwość dodawania własnych komentarzy tekstowych.

3.7.13 System powinien umożliwiać operatorom modyfikację domyślnego menu komentarzy za pomocą bardziej odpowiednich komentarzy niestandardowych.

3.7.14 System powinien umożliwiać operatorom elektroniczną eskalację alarmu do "sprawy" oraz wyznaczenie osób do przeprowadzenia dochodzenia, a tym samym zaalarmowanie i zaangażowanie struktur zarządzania ochroną.

3.7.15 System powinien umożliwiać operatorom filtrowanie alarmów historycznych przy użyciu powiązanych z nimi zapisów i metadanych. Parametry filtrowania powinny obejmować:

3.7.15.1 Alarmy, sesje (gdzie wiele alarmów mogło zostać przesłanych w ramach jednego połączenia).

3.7.15.2 Operator sterowni (na podstawie informacji o logowaniu).

3.7.15.3 Przypadki (alarmy, w przypadku których nastąpiła eskalacja do dalszego badania).

3.7.16 System powinien umożliwiać operatorom dwukrotne kliknięcie wpisu (Alarm, Sesja, Login operatora, Sprawa) w interfejsie alarmów historycznych w celu wyświetlenia bardziej szczegółowego ekranu informacji/działania związanego z tym wpisem, na którym powinna istnieć możliwość wykonania następujących czynności:

3.7.16.1 Wyświetlenie nazwy miejsca alarmowania.

3.7.16.2 Wyświetlenie nazwy serwera alarmowego.

3.7.16.3 Wyświetlenie opisu alarmu.

3.7.16.4 Wyświetlanie operatora sterowni, który obsługiwał alarm lub sesję.

3.7.16.5 Wyświetlenie nazwy jednostki dyspozytorskiej, przez którą obsługiwany był alarm lub sesja.

3.7.16.6 Wyświetlanie czasu wystąpienia zdarzenia alarmowego.

3.7.16.7 Wyświetlenie czasu, w którym zdarzenie alarmowe zostało wysłane do dyspozytorni.

3.7.16.8 Wyświetlenie czasu dotarcia alarmu do dyspozytorni.
3.7.16.9 Podgląd czasu potrzebnego na obsłużenie alarmu przez Operatora dyspozytorni.
3.7.16.10 Przeglądanie komentarzy związanych z alarmami, sesjami i sprawami.
3.7.16.11 Przeglądanie nagrań powiązanych z alarmem.
3.7.16.12 Nawiązanie połączenia z historyczną lokalizacją alarmowania w celu pobrania dalszych nagrań związanych z alarmem, jeśli nadal istnieją w bazie danych lokalizacji zdalnej.
3.7.16.13 Przeglądanie spraw związanych z alarmem.
3.7.16.14 Wyświetlanie całej sesji, w której obsługiwany był alarm.
3.7.16.15 Dodawanie dalszych komentarzy do historycznych alarmów, sesji i przypadków.
3.7.16.16 Eskalacja alarmu historycznego do sprawy w celu dalszego zbadania i rozwiązania.
3.7.16.17 Wyświetlanie loginów Operatora sterowni powiązanych z sesją alarmową.
3.7.16.18 Wyświetlanie wszystkich alarmów powiązanych z sesją.
3.7.16.19 Wyświetlenie czasu trwania, godziny rozpoczęcia i zakończenia logowania Operatora Sali Kontrolnej.
3.7.16.20 Wyświetlenie liczby sesji obsługiwanych przez Operatora w czasie Logowania.
3.7.16.21 Wyświetlenie wszystkich sesji obsługiwanych przez Operatora w czasie Logowania.
3.7.16.22 Wyświetlenie opisu Sprawy.
3.7.16.23 Wyświetlenie nazwy użytkownika, który eskalował alarm do Sprawy wraz z datą i godziną.
3.7.16.24 Wyświetlenie nazwy użytkownika, który zamknął Sprawę, wraz z datą i godziną.
3.7.16.25 Wyświetlenie listy użytkowników Sprawy, wraz z ich Statusem odnoszącym się do Sprawy (Aktywny - nadal nad nią pracuje lub Nieaktywny - nie pracuje już nad nią).
3.7.16.26 Wyświetlanie osi czasu działań użytkownika związanych z daną Sprawą.
3.7.16.27 Przeglądanie statusu Sprawy.
3.7.16.28 Wyświetlanie wszystkich alarmów powiązanych ze Sprawą.
3.7.16.29 Wyświetlanie wszystkich komentarzy powiązanych ze Sprawą
3.7.17 System powinien dostarczać raporty, które mogą być dostosowywane do potrzeb klientów.

3.8 Interfejs programowania aplikacji

3.8.1 System powinien zawierać interfejs programowania aplikacji (API) umożliwiający oprogramowaniu osób trzecich pobieranie informacji z systemu VMS i zarządzanie nimi, a także kontrolę zasobów systemu.
3.8.2 System ogranicza dostęp do obiektu za pomocą uwierzytelnienia skróconego oraz w oparciu o wstępnie skonfigurowane poziomy dostępu użytkownika.
3.8.3 System powinien umożliwiać wyświetlanie listy wszystkich kamer i zasobów kamer w danym obiekcie. Uwaga: kanały z formatami wideo, które nie są obsługiwane przez RTSP będą wyłączone z listy kamer API.
3.8.4 System powinien zawierać informacje identyfikujące zasilanie kamery, takie jak nazwa, unikalny identyfikator, zasilanie dźwiękowe (tak/nie), informacje o poziomie dostępu, status kamery "Online/Offline", status PTZ, informacje o wzorcach/ustawieniach wstępnych, informacje o ścieżce wideo na żywo i do wglądu.
3.8.5 System powinien umożliwiać strumieniowe przesyłanie obrazu wideo z kamery na żywo i przeglądanie przy użyciu protokołu RTSP.
3.8.6 System powinien wymagać uwierzytelnienia klienta w przypadku strumieniowej transmisji obrazu na żywo.
3.8.7 System powinien obsługiwać następujące rodzaje transportu strumieniowego:

3.8.7.1 RTP over UDP.

3.8.7.2 RTP przez TCP.

3.8.8 System powinien umożliwiać strumieniowanie niezależnych wejść i wyjść audio do i z wejść i wyjść audio na serwerze za pomocą protokołu SIP.

3.8.9 System powinien umożliwiać sterowanie kamerami PTZ.

3.8.10 System powinien monitorować i aktualizować na żądanie wszystkie aktualne wejścia i wyjścia z obiektu.

3.8.11 System powinien umożliwiać odbieranie z serwera alarmów technicznych i alarmów o zdarzeniach.

3.8.12 System powinien posiadać interfejs osi czasu.