Specyfikacja CathexisVision 2020 A&E

Spis treści

1 Wprowadzenie

W niniejszym dokumencie przedstawiono ogólne wymagania dotyczące oprogramowania CathexisVision Video Management Software (które może być dalej określane jako "VMS") i/lub urządzeń peryferyjnych produkowanych przez Cathexis Technologies i dostarczanych przez dystrybutorów Cathexis w wybranych regionach.[1]

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 Ogólne wymagania systemowe

Architektura systemu

2.1.1 Systemem powinien być system nadzoru wizyjnego CathexisVision.

2.1.2 System powinien mieć charakter korporacyjny i umożliwiać zdalne zarządzanie wieloma lokalizacjami.

2.1.2.1 System powinien zapewniać kompletną, zdalną konfigurację i klienta konserwacji.

2.1.2.2 System nie powinien opierać się na aplikacjach zdalnego pulpitu do zdalnego połączenia.

2.1.3 System powinien obsługiwać szyfrowanie wszystkich połączeń ze stronami zewnętrznymi.

2.1.3.1 System powinien oferować cztery poziomy szyfrowania:

2.1.3.1.1 Wyłączone,

2.1.3.1.2 Minimalny - szyfrowane będą tylko połączenia krytyczne,

2.1.3.1.3 Secure (domyślny) - szyfrowane są wszystkie połączenia z wyjątkiem tych, w których występuje duża ilość materiału wideo,

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

2.1.3.2 Silnik szyfrujący powinien wykorzystywać szyfry openssl (SHA512 hashes, ephemeral DH-RSA with forward secrecy (DH 2048 bit) oraz AES-GCM 128-bit symmetric ciphers) równoważne TLS 1.3.

2.1.4 System nie powinien wymagać dedykowanego serwera zarządzającego, dzięki czemu wymaga mniejszej ilości sprzętu.

2.1.5 System nie powinien wymagać dedykowanej bazy danych SQL do zapisu.

2.1.6 System powinien mieć charakter "klient/serwer" i składać się z następujących elementów:

2.1.6.1 Serwery zarządzające zapisem.

2.1.6.2 Stacje podglądu i zarządzania dla klientów znajdujących się na miejscu i poza nim.

2.1.6.3 Zewnętrzne klienty telefonów komórkowych/tabletów.

2.1.6.4 Serwer zarządzania alarmami.

2.1.7 System powinien być przystosowany do pracy w środowiskach systemów operacyjnych Windows (32/64-bitowych) lub Linux.

2.1.8 System powinien być zdolny do pracy w środowisku maszyn wirtualnych.

2.1.8.1 System powinien mieć świadomość pracy w środowisku serwerów wirtualnych oraz posiadać wiedzę na temat sprzętu będącego ich podstawą.

2.1.9 System powinien posiadać licencje na użytkowanie z zastosowaniem różnych licencji dla całego obiektu.

2.1.9.1 System powinien być łatwo rozszerzalny poprzez dodanie kamer IP, integracji systemów innych firm, analityki wideo i/lub licencji sprzętowych systemu analogowego.

2.1.9.2 System powinien zapewniać pewne wbudowane funkcje, które mogą być odblokowane do użytku za pomocą klucza programowego, umożliwiając szybką aktywację wymaganych funkcji.

2.1.9.3 Powinna istnieć możliwość łatwej aktualizacji systemu do nowszych wersji za pomocą płyty CD, klucza USB lub innych podobnych środków.

2.1.10 System powinien być łatwy do rozbudowy poprzez dodanie serwerów zapisu, przeglądania i zarządzania oraz pamięci masowej.

Konfiguracja systemu

2.1.11 System powinien umożliwiać zdalne połączenie z systemem poprzez ADSL, VPN lub inne źródło komunikacji.

2.1.11.1 System powinien umożliwiać wykonywanie wszystkich funkcji konfiguracji i podglądu poprzez to zdalne połączenie.

2.1.12 System powinien przechowywać pełną konfigurację obiektu na miejscu lub poza nim w celu odtworzenia w przypadku awarii dysku twardego.

2.1.12.1 System powinien umożliwiać łatwe przywrócenie tej konfiguracji.

2.1.13 System powinien prowadzić dzienniki aktywności użytkowników.

2.1.14 System powinien umożliwiać synchronizację czasową wszystkich podsystemów w obiekcie.

2.1.15 System powinien zarządzać nieograniczoną liczbą wejść i wyjść przekaźnikowych.

2.1.16 System powinien udostępniać kreatory ustawień umożliwiające szybkie, proste dodawanie i konfigurowanie określonych urządzeń i obiektów, takich jak kamera, urządzenia zintegrowane, mapy terenu itp.

2.1.17 System powinien wykorzystywać technologie Universal Plug and Play (UPnP) oraz ONVIF Device discovery do wykrywania urządzeń IP oraz pobierania ustawień z tych urządzeń.

2.1.18 System powinien pobierać i przechowywać lokalnie wszystkie zasoby obiektu, mapy i inne parametry specyficzne dla obiektu, aby zapewnić szybki dostęp i zarządzanie przepustowością dla zdalnych połączeń klienckich. Jeśli zostały one zmodyfikowane w miejscu instalacji, należy je ponownie załadować z miejsca instalacji do zdalnego połączenia klienckiego po ponownym nawiązaniu połączenia.

Możliwości audio i wideo

2.1.19 Ogólny system nie powinien mieć ograniczeń co do liczby kamer/ strumieni wideo.

2.1.20 System powinien być cyfrowym systemem zapisu obrazu i dźwięku oraz zdalnego monitoringu z możliwością jednoczesnego wyświetlania, zapisu, odtwarzania, wyszukiwania i przesyłania obrazu i dźwięku.

2.1.21 System powinien mieć charakter prawdziwie hybrydowy i powinien być zdolny do obsługi następujących źródeł wideo:

2.1.21.1 Kamery wideo IP.

2.1.21.1.1 Należy dostarczyć oddzielną listę obsługiwanych kamer IP lub listę zamieszczoną na stronie internetowej CathexisVision.

2.1.21.2 Enkodery wideo IP (Cathexis i innych producentów).

2.1.21.3 Analogowe systemy wizyjne Cathexis.

2.1.21.4 Urządzenia zgodne z normą ONVIF.

2.1.22 Każdy serwer zarządzania zapisem powinien być zdolny do zarządzania wieloma strumieniami wideo z kamer IP, ograniczonymi jedynie możliwościami przetwarzania sprzętu oraz dostępną lokalną/zdalną pamięcią masową systemu.

2.1.23 System powinien obsługiwać połączenia https do sterowania kamerami, o ile są one dostarczane przez producenta kamer.

2.1.24 System powinien obsługiwać szyfrowany obraz wideo, jeśli jest on dostarczany przez producenta kamery.

3 Strumieniowe przesyłanie wideo i audio

Możliwości ogólne

3.1.1 System powinien zarządzać strumieniową transmisją na żywo, nagrywaniem i przeglądaniem obrazu i dźwięku z różnych źródeł.

Strumieniowa transmisja wideo

3.1.2 System powinien umożliwiać jednoczesne zarządzanie obrazem z analogowych kart wizyjnych i źródeł wizyjnych IP.

3.1.3 System powinien umożliwiać jednoczesne zarządzanie strumieniami MJPEG, MPEG4, H264, H265 i MxPEG oraz ich kombinacją, w zależności od możliwości kamery.

3.1.4 System powinien być w stanie zarządzać strumieniami wizyjnymi typu Unicast lub Multicast.

3.1.5 System powinien umożliwiać kierowanie wybranych strumieni wizyjnych do wybranych monitorów wizyjnych w celu wyświetlania i przeglądania obrazu.

3.1.6 System powinien umożliwiać wyświetlanie obrazu wideo w rozdzielczości HD lub wyższej, jeśli jest to wymagane.

3.1.7 System powinien umożliwiać zarządzanie dynamicznymi strumieniami oraz inteligentny wybór strumienia z kamery w oparciu o rozdzielczość wyświetlacza klienta, serwera i/lub ściany wideo w celu poprawy wydajności podglądu na żywo i zmniejszenia zużycia zasobów.

3.1.8 System powinien umożliwiać "transkodowanie" strumieni wideo do niższej szerokości pasma, na potrzeby monitoringu poza siedzibą firmy (w zależności od dostępności odpowiednich strumieni wideo i mocy obliczeniowej serwerów wideo).

Strumieniowe przesyłanie dźwięku

3.1.9 System powinien umożliwiać odbieranie i przechowywanie zsynchronizowanego dźwięku z kamer z funkcją audio.

3.1.10 System powinien umożliwiać zapis i odtwarzanie zsynchronizowanego dźwięku i obrazu.

3.1.10.1 Zakładając, że źródłowy sygnał audio i wideo jest zsynchronizowany w kamerze, system powinien być w stanie utrzymać tę synchronizację z dokładnością poniżej 500 milisekund.

3.1.11 System powinien umożliwiać zarządzanie dwukierunkowym dźwiękiem, z systemu do zdalnego urządzenia IP lub kamery, z odpowiednimi możliwościami audio.

3.1.12 System powinien umożliwiać strumieniowe przesyłanie/przechowywanie i odtwarzanie nieograniczonej liczby strumieni audio z kamer.

4 Zarządzanie użytkownikami i prawa dostępu

Zarządzanie użytkownikami

4.1.1 System powinien umożliwiać zarządzanie użytkownikami w danej lokalizacji oraz powinien stosować wszystkich użytkowników i ich prawa dostępu do wszystkich serwerów w danej lokalizacji.

4.1.2 System powinien umożliwiać administratorom konfigurację użytkowników w obiekcie oraz przypisywanie im nazw użytkowników, poziomów dostępu i haseł.

4.1.2.1 System powinien posiadać trzydzieści poziomów użytkowników, przy czym najwyższy poziom w hierarchii to 30, a najniższy poziom w hierarchii to 1.

4.1.3 System powinien umożliwiać nadawanie poszczególnym użytkownikom serwisu uprawnień do:

4.1.3.1 Przeglądania wszystkich zasobów witryny.

4.1.3.2 Zdalnego łączenia się.

4.1.3.3 Zmiany własnego hasła.

4.1.4 Dostęp do systemu powinien być realizowany na podstawie nazwy użytkownika i hasła, a wszystkie działania użytkownika powinny być rejestrowane w odniesieniu do jego nazwy w ścieżce audytu operatora. Ta ścieżka audytu powinna być dostępna, możliwa do wydrukowania i możliwa do kontroli dostępu.

LDAP/aktywne katalogi

4.1.5 System powinien umożliwiać import użytkowników z systemu zarządzania użytkownikami LDAP (Lightweight Directory Access Protocol) tylko na stronach Professional i Premium.

4.1.6 System powinien umożliwiać przypisywanie praw dostępu do VMS zaimportowanym użytkownikom LDAP.

4.1.7 System powinien wykorzystywać LDAP do komunikacji z systemami zarządzania użytkownikami takimi jak Active Directory i OpenLDAP.

4.1.8 Przy każdym logowaniu użytkownika zarejestrowanego w systemie LDAP system powinien odpytywać serwer systemu zarządzania o ważność danych uwierzytelniających.

4.1.9 Logowanie użytkowników LDAP przy użyciu mobilnych We/Wy lub API systemu nie będzie dozwolone ani walidowane.

Prawa dostępu

4.1.10 System powinien umożliwiać ograniczanie dostępności zasobów serwisu dla użytkowników na podstawie praw dostępu nadanych im przez administratorów.

4.1.11 System powinien umożliwiać administratorom przypisywanie praw dostępu do poziomów użytkowników, lokalnie lub zdalnie.

4.1.12 System ogranicza dostęp do zakładki setup (w której dokonywana jest konfiguracja obiektu, np. konfiguracja, podgląd i kontrola baz danych, kamer, analityki wideo itp.

4.1.13 System powinien umożliwiać administratorom nadawanie użytkownikom następujących praw dostępu do zasobów witryny (takich jak kamery, wejścia/wyjścia, monitory, itp.):

4.1.13.1 Podgląd na żywo.

4.1.13.2 Przegląd.

4.1.13.3 Sterowanie ręczne PTZ, opcje menu PTZ, ustawianie presetów PTZ, sterowanie trasami PTZ.

4.1.13.4 Odsłuch audio.

4.1.13.5 Ukrywanie stref prywatności.

4.1.13.6 Eksport danych.

4.1.13.7 Resetowanie sabotażu kamery.

5 Nagrywanie, archiwizacja i przechowywanie

Zapis

5.1.1 System powinien umożliwiać:

5.1.1.1 Częstotliwość zapisu klatek na sekundę większa niż 30, w zależności od możliwości kamery.

5.1.1.2 Zapis do różnych, skonfigurowanych baz danych.

5.1.1.3 Nagrania inicjowane przez użytkownika. Użytkownicy z odpowiednimi prawami dostępu mogą ręcznie wyzwalać nagrywanie.

5.1.1.4 Nagrywanie zdarzeń. Zdarzenia mogą być skonfigurowane w taki sposób, aby wyzwalały nagrywanie na odpowiedniej kamerze.

5.1.1.5 Zaplanowane nagrania. Kamery mogą być ustawione na nagrywanie według ustalonego harmonogramu.

5.1.1.6 Zapis ciągły. Urządzenia (takie jak urządzenia zintegrowane i kamery) są nagrywane w sposób ciągły i tworzą znaczniki czasu w nagraniu.

5.1.1.7 Prosty zapis ruchu. Konfigurowalny za pomocą kreatora konfiguracji kamery lub oddzielnie.

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

5.1.2 System powinien udostępniać funkcję nagrywania ekranu, która umożliwia nagrywanie dowolnego ekranu komputera podłączonego do dowolnego komputera z systemem Windows/Linux. Będzie to nagrywane do systemu VMS tak, jakby była to standardowa kamera IP.

Archiwizacja (eksport)

5.1.3 System powinien posiadać następujące możliwości archiwizacji wideo:

5.1.3.1 Eksportowanie audio i wideo z oprogramowania w zastrzeżonym formacie wideo, z opcjonalnym samodzielnym odtwarzaczem.

5.1.3.2 Oznaczanie czasu rozpoczęcia i zakończenia archiwizowanego materiału wideo.

5.1.3.3 Archiwizacja wielu kamer jednocześnie.

5.1.3.4 Zachowanie w archiwum wszystkich metadanych wideo widocznych w momencie archiwizacji.

5.1.3.5 Archiwizacja wybranych materiałów z jednej lub wielu kamer na płyty DVD, pamięci USB, lokalne lub zdalne dyski twarde w formatach dozwolonych przez system operacyjny.

5.1.3.6 Zapisywanie "odtwarzacza" archiwum wraz z materiałem wideo.

5.1.3.7 Archiwizacja i przeglądanie plików zawierających znaki inne niż ASCII (np. arabskie).

5.1.3.8 Eksportowanie materiału wideo z archiwum.

5.1.3.8.1 System powinien umożliwiać eksport wideo z archiwum w formacie MP4 lub archiwalnym.

5.1.3.8.2 System powinien umożliwiać wybór zarchiwizowanych kamer, które mają być uwzględnione w eksporcie.

5.1.3.9 System powinien zapewniać możliwość wykonania zaplanowanej archiwizacji w następujący sposób:

5.1.3.9.1 Archiwizacja wybranych kamer.

5.1.3.9.2 Archiwizacja tylko wybranego okresu zarejestrowanego materiału.

5.1.3.9.3 Archiwizacja o wybranej porze dnia.

5.1.4 System powinien posiadać następujące zabezpieczenia w zakresie archiwizacji obrazu i eksportu obrazu z archiwum:

5.1.4.1 Możliwość archiwizacji powinna być funkcją kontrolowaną prawami dostępu.

5.1.4.2 System powinien umożliwiać administratorom tworzenie na poziomie użytkownika "profili archiwizacji", dla których konfigurowane są hasła i znaki wodne.

5.1.4.2.1 W zależności od hasła i opcji archiwizacji skonfigurowanych w danym profilu archiwizacji, system powinien wymagać od użytkowników ustanowienia hasła i/lub zastosowania znaku wodnego przy archiwizacji wideo.

5.1.4.2.2 Dla celów ścigania i innych celów prawnych, zarchiwizowane obrazy powinny być podpisane cyfrowo unikalnym identyfikatorem oryginalnego serwera archiwizacji, który jest tracony w przypadku próby manipulacji obrazem.

5.1.4.2.3 System powinien umożliwiać ograniczenie możliwości eksportu z archiwum.

5.1.4.2.3.1 System powinien usuwać sygnaturę serwera z wideo wyeksportowanego z archiwum w formacie MP4.

5.1.5 System powinien umożliwiać przeglądanie zarchiwizowanych materiałów wideo z poziomu oprogramowania, jak również z poziomu samodzielnego "odtwarzacza" archiwów (który może być zainstalowany niezależnie). System powinien umożliwiać następujące funkcje przeglądania archiwów:

5.1.5.1 Przeszukiwanie NVR w poszukiwaniu plików archiwalnych.

5.1.5.2 Jednoczesny przegląd wszystkich kamer w archiwum wielokamerowym.

5.1.5.3 Przeglądanie obrazu wideo przy użyciu zwykłych narzędzi do odtwarzania wideo.

5.1.5.4 Przeglądanie wszystkich zdarzeń systemowych związanych z archiwizowanymi kamerami.

5.1.5.5 Wybieranie szablonów układu do wyświetlania zarchiwizowanych kamer.

5.1.5.6 Eksportowanie zrzutów wideo z podaniem nazwy kamery, czasu, tytułu zrzutu oraz dowolnych notatek.

5.1.5.7 Nakładanie wyeksportowanego obrazu zrzutu z nazwą i czasem kamery. System powinien zapisać wybór dokonany przez użytkownika i wykorzystać go do kolejnych eksportów.

5.1.5.8 Płynne skalowanie i usuwanie zniekształceń obrazu wideo.

5.1.5.9 Weryfikacja archiwum pod kątem autentyczności, polegająca na sprawdzeniu archiwum pod kątem unikalnego podpisu cyfrowego oryginalnego serwera archiwizującego.

5.1.5.9.1 Weryfikacja autentyczności archiwów nie jest możliwa w przypadku braku sygnatury oryginalnego serwera archiwizacji.

Przechowywanie danych

5.1.6 System powinien umożliwiać zapisywanie wybranych strumieni wideo do wybranych baz danych wideo.

5.1.6.1 System powinien umożliwiać zapisywanie materiału wideo z tych samych kamer do wielu baz danych jednocześnie.

5.1.7 System powinien umożliwiać tworzenie i zarządzanie wieloma bazami danych.

5.1.8 System powinien umożliwiać zarządzanie bazami danych obejmującymi wiele urządzeń lokalnych lub sieciowych pamięci masowych (NAS).

5.1.9 System powinien umożliwiać dostęp do udziałów sieciowych Windows z poziomu oprogramowania.

5.1.10 System powinien umożliwiać ostrzeganie użytkownika o odłączeniu od zarządzania pamięcią masową dysków/udziałów sieciowych zawierających bazy danych wykorzystywane przez oprogramowanie.

5.1.11 System powinien umożliwiać niszczenie baz danych w celu trwałego zniszczenia nagrań wideo starszych niż maksymalny limit dni nagrań.

6 Graficzny interfejs użytkownika (GUI)

Ogólne możliwości GUI

6.1.1 System powinien udostępniać graficzny interfejs użytkownika (GUI), który umożliwia użytkownikom łatwe przeglądanie wszystkich zasobów (kamery, komponenty audio, bazy danych, wejścia, wyjścia, układy itp.) w całym obiekcie i nie powinien być ograniczony do określonych adresów IP. Sieciowe serwery wizyjne.

6.1.1.1 System powinien udostępniać dwa interfejsy w ramach ogólnego graficznego interfejsu użytkownika: interfejs operatora oraz interfejs konfiguracji.

6.1.1.1.1 System powinien umożliwiać dostęp do interfejsu ustawień, w którym przeprowadzana jest cała konfiguracja lokalizacji, wyłącznie użytkownikom będącym administratorami.

6.1.1.1.2 System powinien umożliwiać wszystkim poziomom użytkowników przeglądanie zasobów dostępnych w interfejsie operatora w różnym stopniu (w zależności od przypisanych im praw dostępu).

6.1.2 System powinien wspierać tłumaczenie GUI na różne języki, w tym:

6.1.2.1 arabski,

6.1.2.2 holenderski,

6.1.2.3 angielski,

6.1.2.4 francuski,

6.1.2.5 węgierski,

6.1.2.6 włoski,

6.1.2.7 portugalski,

6.1.2.8 hiszpański.

6.1.3 Z poziomu interfejsu operatora powinno być możliwe jednoczesne otwieranie wielu witryn i wyświetlanie ich na wybranych monitorach w systemie. Obejmuje to powiązane zasoby obiektów, takie jak mapy obiektów, transmisje z kamer itp.

6.1.4 Graficzny interfejs użytkownika powinien umożliwiać przeglądanie na maksymalnie 6 monitorach z jednego komputera z oprogramowaniem klienckim. Użytkownik powinien mieć możliwość dostosowania monitorów do swoich potrzeb, tak aby mógł oglądać różne elementy (np. mapy, kamery, dane transakcji integracji systemów stron trzecich itp.) na różnych monitorach lub w "zakładkach" okien na tym samym monitorze.

6.1.5 Układ interfejsu operatora powinien być konfigurowalny, jak w poniższym przykładzie:

6.1.5.1 Funkcje systemu lub funkcje, które nie są aktywowane, lub do których użytkownik nie ma dostępu, powinny być ukryte przed wzrokiem - użytkownik powinien widzieć tylko funkcje, z których korzysta.

6.1.5.2 Zasoby, do których użytkownik nie ma dostępu, są dla niego niedostępne.

6.1.5.3 Lokalizacja panelu zasobów może być ustawiona po prawej lub lewej stronie ekranu zakładki kamery.

6.1.6 System powinien udostępniać pasek stanu w dolnej części GUI, wskazujący informacje o oprogramowaniu za pomocą ikon stanu, z których każda może być kliknięta w celu uzyskania dalszych informacji. Na przykład:

6.1.6.1 System powinien pokazywać ostrzeżenie o licencji dla zasobów witryny, które są nieprawidłowo licencjonowane.
6.1.6.2 System powinien wyświetlać nazwę użytkownika i poziom dostępu zalogowanego użytkownika.
6.1.6.3 System powinien wyświetlać zastosowaną licencję witryny.
6.1.6.4 W przypadku awarii kamery system powinien wyświetlić powiadomienie o kamerze.
6.1.6.5 System powinien wyświetlać monitor wydajności, który wskazuje statystyki wydajności systemu.
6.1.6.6 System powinien wyświetlać status połączenia aktualnej jednostki z obiektem.
6.1.6.7 System powinien wyświetlać powiadomienie o analizie wideo w przypadku wystąpienia błędu w jednym lub kilku kanałach wizyjnych obiektu.
6.1.6.8 System powinien wyświetlać powiadomienie o awarii, które zawiera informacje o stanie istniejących serwerów awaryjnych.
6.1.6.9 System powinien wyświetlać ostrzeżenie o sabotażu, gdy uznano, że nastąpił sabotaż co najmniej jednej z kamer w obiekcie.

Kamery

6.1.7 Interfejs konfiguracyjny
6.1.7.1 System powinien ograniczać dostęp do konfiguracji kamer w miejscu instalacji w interfejsie ustawień do administratorów.
6.1.7.2 System powinien udostępniać kreatora dodawania i konfigurowania kamer.
6.1.7.3 System powinien umożliwiać konfigurację nagrań planowych, nagrań ruchu oraz nagrań analitycznych z poziomu kreatora konfiguracji.
6.1.7.4 System powinien zapewniać funkcję "kopiuj i wklej", która umożliwia użytkownikom łatwe kopiowanie ustawień kamery, w tym informacji z wielu strumieni wideo, do wielu kamer.
6.1.7.5 Podczas konfiguracji kamery system powinien wyświetlać adres URL/stronę internetową kamery, którą można załadować do przeglądarki.
6.1.7.6 System powinien umożliwiać administratorowi oznaczenie kamery jako "ukrytej". W takim przypadku kamera powinna być widoczna i przeglądana/przeglądana tylko przez administratorów.
6.1.7.7 System powinien obsługiwać automatyczne skalowanie wysokiego DPI.
6.1.7.8 System powinien udostępniać raporty dotyczące kamer pracujących w trybie online oraz off-line (uszkodzonych).

6.1.8 Interfejs operatora
6.1.8.1 System powinien umożliwiać użytkownikom podgląd i współpracę z kamerami w różnym stopniu, w zależności od przydzielonych praw dostępu.
6.1.8.2 System powinien umożliwiać użytkownikowi wybór określonych kamer, które mają być oglądane na wybranych monitorach lub wybranych panelach w obrębie wybranych monitorów.
6.1.8.3 System powinien zapewniać możliwość przeciągania kamer z panelu zasobów na wybrane monitory lub panele na monitorze.
6.1.8.4 System powinien umożliwiać synchronizację kamer podczas odtwarzania.
6.1.8.5 System powinien umożliwiać użytkownikom wstrzymanie odtwarzania obrazu wideo i jego wydrukowanie, skopiowanie do schowka lub zapisanie obrazu w wybranym miejscu.

6.1.8.6 System powinien umożliwiać użytkownikom przeciąganie kamer z mapy do wybranych monitorów lub paneli na monitorze.

6.1.8.7 System powinien umożliwiać konfigurację i inicjowanie tras (sekwencji) kamer na wybranych monitorach lub na panelach w obrębie wybranego monitora.

6.1.8.8 System powinien zapewniać możliwość tworzenia i zapisywania wielu "układów" kamer, które mogą być następnie łatwo wybierane, ręcznie przez użytkownika lub automatycznie w przypadku wystąpienia zdarzenia.

6.1.8.9 System powinien umożliwiać inicjowanie tras (sekwencji) "układów" (zwanych również "salwą") na wybrane monitory.

6.1.8.10 System powinien umożliwiać użytkownikowi De-warp video z kamer panoramicznych 180 lub 360 stopni.

6.1.8.11 System powinien umożliwiać użytkownikowi podgląd do 64 kamer na jednym monitorze.

6.1.8.12 System powinien umożliwiać użytkownikom cyfrowe powiększanie obrazu z poszczególnych kamer.

6.1.8.13 System powinien umożliwiać użytkownikom wybór strumienia, który ma być wyświetlany, jeśli do podglądu na żywo wyznaczono wiele strumieni kamer.

Zasoby terenu

6.1.9 System powinien umożliwiać administratorom konfigurację zasobów obiektu, które są widoczne w interfejsie operatora.

6.1.10 System powinien umożliwiać administratorom tworzenie folderów i przydzielanie zasobów do wybranych folderów.

6.1.11 Dostęp użytkownika do zasobów serwisu powinien być kontrolowany za pomocą nazwy użytkownika i hasła, zarówno w przypadku podglądu lokalnego, jak i zdalnego, ograniczonego poziomem dostępu poszczególnych użytkowników.

6.1.12 Użytkownik powinien mieć możliwość zobaczenia wyzwalaczy wejścia z GUI.

6.1.13 Użytkownik powinien mieć możliwość sterowania wyjściami z graficznego interfejsu użytkownika.

Nakładki tekstowe i graficzne

6.1.14 Interfejs operatora powinien opcjonalnie wyświetlać informacje graficzne z urządzeń krajowych i urządzeń innych producentów w formie nakładek na panele kamer.

6.1.15 System powinien umożliwiać zmianę położenia bloków nakładek oraz zmianę rozmiarów nakładek, rozmiarów tekstu, przezroczystości i koloru.

6.1.16 Interfejs operatora powinien mieć możliwość opcjonalnego pokazywania działania algorytmów analitycznych poprzez wyświetlanie nakładek.

Sterowanie PTZ

6.1.17 System powinien umożliwiać sterowanie kamerami PTZ (Pan-Tilt-Zoom) z poziomu interfejsu operatora oraz za pomocą działań związanych ze zdarzeniami.

6.1.18 System powinien także umożliwiać użytkownikom sterowanie kamerami PTZ za pomocą dołączonej klawiatury/joysticka.

6.1.19 Sterowanie PTZ obejmuje:

6.1.19.1 Obrót, pochylenie i zoom.

6.1.19.2 Zmienną prędkość ruchu PTZ.

6.1.19.3 Sterowanie ostrością i przysłoną.

6.1.19.4 Definiowanie zaprogramowanych pozycji kamery PTZ.

6.1.19.5 Przypisywanie unikalnych nazw do zaprogramowanych pozycji kamery PTZ.

6.1.19.6 Przejście do pozycji domyślnych kamery PTZ.

6.1.20 System powinien umożliwiać priorytetowe sterowanie kamerą PTZ.

6.1.20.1 Użytkownik administrator ma najwyższy priorytet sterowania kamerą PTZ, po czym hierarchia priorytetów biegnie w dół od poziomu użytkownika 30 do poziomu użytkownika 1.

6.1.20.2 Dwóch użytkowników na tym samym poziomie będzie miało pierwszeństwo sterowania pierwszym użytkownikiem, a drugi użytkownik musi poczekać, aż upłynie czas "Dome override" (Zastąpienie kamery).

Podgląd na żywo

6.1.21 System powinien umożliwiać użytkownikom podgląd i wstrzymywanie kamer na żywo (w zależności od przydzielonych praw dostępu).

6.1.22 System powinien umożliwiać podgląd na żywo i jednoczesne odtwarzanie określonych kamer oraz ich synchronizację, jeśli jest to wymagane.

6.1.23 System powinien umożliwiać podgląd tej samej kamery na żywo na wielu monitorach lub panelach na jednym monitorze.

6.1.24 System powinien umożliwiać wyświetlanie ścieżek aktywności przez maksymalnie 15 minut w trybie podglądu na żywo. Patrz punkt 7.10.

Przeglądanie

6.1.25 System powinien umożliwiać przegląd kamer w tym samym oknie i panelu, w którym odtwarzany jest obraz na żywo, bez konieczności otwierania osobnego okna lub karty przeglądu lub bazy danych.

6.1.25.1 System powinien umożliwiać użytkownikom odtwarzanie zarejestrowanego materiału filmowego poprzez kliknięcie i przeciągnięcie osi czasu kamery do żądanego punktu przeglądu.

6.1.25.2 System powinien umożliwiać użytkownikom łatwy przegląd dowolnej kamery w systemie, z dowolnego/wielu klientów podłączonych do systemu, zarówno poza siedzibą, jak i na miejscu.

6.1.26 Jeżeli wybrana kamera została skonfigurowana do zapisu w wielu bazach danych, system powinien wyświetlać użytkownikowi monit o wybranie bazy danych, z której ma być dokonany przegląd.

6.1.27 System powinien umożliwiać przeglądanie nagrań z pokładowych rejestratorów Edge obsługiwanych kamer.

6.1.28 System powinien umożliwiać jednoczesny przegląd wielu kamer oraz synchronizację czasów przeglądów tych kamer.

6.1.29 System powinien zachowywać czasy przeglądów dla różnych kamer wybranych dla tego samego panelu. Jeśli kamera jest w trybie przeglądu, a nowa kamera zostanie otwarta w tym panelu, nowa kamera przejdzie do tego samego czasu przeglądu, co oryginalna kamera.

6.1.30 System powinien kontrolować prawa dostępu do archiwizacji i przeglądania zarchiwizowanych materiałów wideo.

6.1.31 System powinien umożliwiać wykonywanie inteligentnych wyszukiwań z wykorzystaniem następujących narzędzi przeglądowych:

6.1.31.1 Snap-Search. Patrz punkt 6.8.

6.1.31.2 Przeszukiwanie obszaru ruchu. Patrz: sekcja 7.11.

6.1.31.3 Wyświetlanie podglądu miniatur obrazu nagrania po najechaniu myszą na oś czasu.

6.1.32 System powinien umożliwiać wyświetlanie ścieżek aktywności dla maksymalnie 60 minut w trybie przeglądania. Patrz punkt 7.10.

Strefy prywatności

6.1.33 System powinien umożliwiać użytkownikom-administratorom tworzenie i usuwanie stref prywatności w obrazie z kamery.

6.1.33.1 Strefy prywatności powinny być konfigurowalnymi czarnymi wielokątami, które zasłaniają wrażliwe obszary obrazu z kamery.

6.1.34 System powinien pokazywać strefy prywatności na żywo, podczas przeglądania i archiwizacji materiału wideo.

6.1.35 System powinien pozwalać użytkownikom z odpowiednimi prawami dostępu na ukrywanie/pokazywanie stref prywatności.

6.1.36 System powinien pokazywać/ukrywać strefy prywatności w zarchiwizowanym materiale filmowym w zależności od tego, czy zostały one ukryte/pokazane przez użytkownika w momencie archiwizacji.

Narzędzia inteligentnego wyszukiwania do przeglądania

6.1.37 System powinien umożliwiać inteligentne przeszukiwanie przeglądanego materiału wideo pod kątem ruchu z wykorzystaniem danych zebranych z Motion Database. Narzędziami tymi są:

6.1.37.1 Snap-Search:

6.1.37.1.1 W przeglądzie system powinien być zdolny do podzielenia zdefiniowanego przez użytkownika okresu czasu na zdefiniowaną przez użytkownika macierz miniatur obrazów.

6.1.37.1.2 System powinien umożliwiać użytkownikowi zawężenie zdefiniowanego okresu wyszukiwania pomiędzy wyświetlanymi miniaturami poprzez kliknięcie i przeciągnięcie pomiędzy żądanymi miniaturami.

6.1.37.1.3 Macierz miniatur zostanie ponownie skonfigurowana dla tego nowego okresu wyszukiwania.

6.1.37.1.4 System powinien umożliwiać definiowanie przedziałów czasowych wyszukiwania według sekund, minut, godzin, dni i tygodni.

6.1.37.1.5 System powinien umożliwiać odtwarzanie zarejestrowanego materiału filmowego począwszy od danej miniatury zarówno w odtwarzaczu wideo interfejsu operatora, jak i w osadzonym odtwarzaczu wideo okna Snap-Search.

6.1.37.1.6 System powinien umożliwiać archiwizację obrazu wideo z poziomu wbudowanego odtwarzacza wideo w oknie Snap-Search.

6.1.37.2 Motion Search:

6.1.37.2.1 W przeglądzie system powinien mieć możliwość wyboru określonych obszarów obrazu z kamery w celu wyszukania ostatniego ruchu w wybranym obszarze.

6.1.37.2.2 System wykorzystuje dane o ruchu zgromadzone w bazie danych o ruchu w celu wskazania ostatniego ruchu w wybranym obszarze.

6.1.37.2.3 System powinien wyświetlać cały ruch w wybranym obszarze w postaci czerwonych pasków ruchu wzdłuż osi czasu przeglądu kamery; im wyższy pasek ruchu, tym większy ruch w wybranym obszarze w danym momencie nagrania.

Ścieżki aktywności:

6.1.38 System powinien umożliwiać wyświetlanie, gdzie i jak niedawno wystąpiła aktywność w różnych obszarach obrazu z kamery, poprzez wyświetlanie nakładek ścieżek aktywności.

6.1.39 System wykorzystuje dane o ruchu zgromadzone w bazie danych Motion Database oraz nagrania z kamer do generowania ścieżek aktywności.

6.1.40 System powinien wyświetlać nakładki ścieżek aktywności w kolorach od zielonego do czerwonego, aby wskazać przeszłą i obecną aktywność w danym obszarze.

6.1.40.1 Im bardziej zielona jest nakładka, tym dalej w czasie wystąpiła aktywność w danym obszarze.

6.1.40.2 Im bardziej czerwona nakładka, tym bardziej aktualna jest aktywność w tym obszarze.

6.1.41 System powinien wyświetlać czas aktywności (w minutach i sekundach) w górnej części nakładki ścieżki aktywności, aby wskazać, jak daleko wstecz od bieżącego czasu miała miejsce aktywność w tym obszarze.

6.1.42 System powinien umożliwiać wyświetlanie nakładek ścieżek aktywności dla pewnych okresów czasu, które są określane na podstawie trybu przeglądania i nagrań z kamery;

6.1.42.1 W trybie podglądu na żywo i/lub jeśli nie skonfigurowano nagrań z kamer, system jest w stanie wyświetlać ścieżki aktywności dla aktywności, która miała miejsce w ciągu ostatnich 15 minut bieżącego czasu.

6.1.42.2 W trybie podglądu (pod warunkiem, że skonfigurowano zapisy z kamer) system jest w stanie wyświetlać ścieżki aktywności dla działań, które miały miejsce w ciągu ostatnich 60 minut bieżącego czasu.

6.1.43 System powinien umożliwiać włączanie i wyłączanie ścieżek aktywności.

6.1.44 System powinien umożliwiać przełączanie się na czas aktywności wskazywany przez nakładkę ścieżki aktywności poprzez dwukrotne kliknięcie na wybranej nakładce ścieżki aktywności.

6.1.45 System powinien wyświetlać ruch w obrazie z kamery w postaci czerwonych pasków ruchu wzdłuż osi czasu przeglądu kamery; im wyższy pasek ruchu, tym większy ruch w obrazie z kamery w danym momencie nagrania

Mapy cieplne

6.1.46 System powinien umożliwiać wyświetlanie nakładki mapy cieplnej z wykorzystaniem danych zestawionych z bazy danych o ruchu w celu wskazania obszarów ruchu.

6.1.47 System powinien wyświetlać obszary o większym lub mniejszym ruchu, wykorzystując spektrum kolorów, odpowiednio od czerwonego do zielonego.

6.1.48 System powinien umożliwiać dopracowanie wyników mapy cieplnej przy użyciu określonych parametrów:

6.1.48.1 Okres analizy, który określa, w jakim czasie kamera będzie analizowana pod kątem ruchu. Okresy analizy obejmują:

6.1.48.1.1 Dzień tygodnia,

6.1.48.1.2 Tydzień miesiąca,

6.1.48.1.3 Miesiąc roku,

6.1.48.1.4 Kwartał roku,

6.1.48.1.5 Rok.

6.1.48.2 Zrzuty wyświetlane w zestawieniu wyników mogą być podzielone według:

6.1.48.2.1 Dzień tygodnia,

6.1.48.2.2 Tydzień miesiąca,

6.1.48.2.3 Miesiąca roku,

6.1.48.2.4 Kwartał roku.

6.1.48.3 Zrzuty wyświetlane w zestawieniu wyników mogą być dostosowywane pod względem wielkości.

6.1.48.4 Nakładki mogą być ustawione tak, aby wyświetlały procent czasu (poza zdefiniowanym okresem analizy), w którym wystąpił ruch.

6.1.48.5 Ustawienia czułości i progu pozwalają na odfiltrowanie ruchu w scenach o wysokim/niskim poziomie aktywności.

Odwzorowanie sąsiednich kamer

6.1.49 System powinien umożliwiać łączenie w oprogramowaniu kamer znajdujących się w fizycznej bliskości, aby umożliwić uproszczoną nawigację między połączonymi kamerami w interfejsie operatora podczas śledzenia obiektów/podejrzanych poruszających się za pomocą wielu kamer.

6.1.50 System powinien udostępniać ekran mapowania umożliwiający konfigurację sąsiednich kamer poprzez wybór kamer z dostępnych zasobów obiektu, które mają być skonfigurowane jako kamery sąsiednie, oraz definiowanie dwukierunkowych relacji między każdą parą sąsiednich kamer.

6.1.51 System powinien umożliwiać zarządzanie kamerami przyległymi przy użyciu "stron", w których do ich organizacji wykorzystywane są foldery i podfoldery.

6.1.51.1 System powinien umożliwiać dodanie tej samej kamery do wielu różnych stron, podfolderów i folderów.

6.1.52 System powinien umożliwiać usunięcie kamery oraz wszystkich powiązanych z nią linków kierunkowych do innych mapowanych kamer:

6.1.52.1 Pojedynczej strony, podfolderu lub folderu bez usuwania jej z innych stron, podfolderów lub folderów; lub

6.1.52.2 Wszystkich stron, podfolderów lub folderów.

6.1.53 W interfejsie operatora system powinien umożliwiać następujące czynności:

6.1.53.1 Wyświetlanie strzałek jako nakładek na skonfigurowane kamery, wskazujących kierunki fizycznie sąsiadujących kamer.

6.1.53.2 Przełączanie na sąsiednie kamery po wybraniu odpowiedniej strzałki sąsiedniej kamery.

6.1.53.3 Umożliwienie użytkownikowi wyboru opcji Kamera przylegająca z menu rozwijanego Zasoby na karcie Kamery.

6.1.53.4 Wyświetlanie sąsiednich kamer po kliknięciu na odpowiednią kamerę w menu rozwijanym Zasoby.

Zakładki

6.1.54 System powinien umożliwiać tworzenie zakładek do przeglądów.

6.1.54.1 Zakładka przechowuje moment w czasie, aby móc go przejrzeć w późniejszym terminie. Dostęp do zapisanej zakładki spowoduje przejście do stanu przeglądu w momencie, w którym została ona zapisana w oprogramowaniu.

6.1.54.2 Zakładki mogą być tworzone dla wielu kamer i są przechowywane dla każdego użytkownika katetoskopu.

6.1.54.3 Zakładki będą różne dla każdego użytkownika zalogowanego do oprogramowania Cathexis.

6.1.54.4 Zakładki będą przechowywane w czasie lokalnego systemu.

6.1.54.5 System powinien przechowywać zakładki lokalnie. Zakładki zapisane na jednej jednostce nie będą dostępne z innej jednostki.

6.1.54.6 Eksport zakładek z kamer może być wykonany 60 minut przed i 60 minut po czasie, w którym zostały one zapisane.

6.1.54.7 Oprogramowanie pozwala na utworzenie archiwum materiału filmowego, które można przeglądać w odtwarzaczu archiwum cathexis.

6.1.54.8 Należy wybrać bazę danych kamer, z której archiwum ma korzystać podczas eksportu.

6.1.54.9 Możliwe jest przywrócenie zakładki z materiału na żywo lub z przeglądu, przy użyciu niestandardowego układu kamery.

6.1.54.10 Zakładka jest ograniczona do 8 kamer w przeglądzie.

6.1.54.11 System powinien pozwalać użytkownikom na tworzenie zakładek tylko z zasobami, do których użytkownik ma dostęp.

6.1.54.12 System nie powinien zapisywać w zakładce:

6.1.54.13 Pozycja PTZ,

6.1.54.14 Aktualnych parametrów zoomu cyfrowego,

6.1.54.15 Sekwencji na żywo uruchomionych w panelu.

6.1.54.16 System nie będzie zabezpieczał danych przed nadpisaniem na serwerze poprzez utworzenie zakładki.

System zarządzania obrazami referencyjnymi

6.1.55 System powinien zapewniać interfejs do tworzenia, utrzymywania i porównywania obrazów referencyjnych (punktów odniesienia) wszystkich kamer na serwerze.

6.1.56 System powinien umożliwiać przeglądanie, eksportowanie lub usuwanie obrazów referencyjnych.

6.1.57 System powinien umożliwiać porównywanie przechwyconych obrazów referencyjnych i/lub aktualnej orientacji kamer serwera.

6.1.58 System powinien wyświetlać różnice pomiędzy porównywanymi obrazami referencyjnymi.

Ściana wizyjna

6.1.59 System powinien zapewniać oprogramowanie Video Wall, które powinno być uruchamiane na komputerach dedykowanych do wyświetlania strumieni wideo.

6.1.60 System powinien umożliwiać wyświetlanie obrazu z wielu kamer w obiekcie na monitorach ściany wideo.

6.1.61 System powinien umożliwiać sterowanie wieloma monitorami podłączonymi do wielu komputerów z jednego punktu poprzez panel MIMIC.

6.1.62 System powinien umożliwiać przeciąganie i upuszczanie kamer na miejsce wyświetlania na ścianie wizyjnej z miejsc innych niż miejsce monitorowania.

6.1.63 System powinien umożliwiać administratorom konfigurację układów kamer ściany wizyjnej, trasy układów (salvo) oraz praw dostępu do ścian wizyjnych.

7 Analityka wideo

Możliwości ogólne

7.1.1 System powinien posiadać własną analitykę i algorytmy wbudowane w oprogramowanie, które mogą być wykorzystywane jako wyzwalacze zdarzeń.

7.1.1.1 Obejmuje to wizyjną detekcję ruchu oraz analizę śledzenia obiektów.

7.1.2 System powinien umożliwiać konfigurację analityki wideo w odniesieniu do nagrań bieżących i zapisanych.

7.1.3 System powinien ograniczać dostęp do konfiguracji analityki tylko do administratorów.

7.1.4 System powinien umożliwiać wykorzystanie analityki wbudowanej w kamerę IP lub nadajnik do inicjowania zdarzeń, z którymi mogą być powiązane wybrane działania.

7.1.5 System powinien umożliwiać integrację z pakietami analitycznymi innych producentów.

7.1.6 System powinien umożliwiać stosowanie następujących funkcji klasyfikacji obiektów w analityce śledzenia obiektów w pakietach analitycznych Basic, Intermediate i Advanced:

7.1.6.1 Klasyfikowanie śledzonych obiektów i wyświetlanie następujących metadanych o klasyfikacji:

7.1.6.1.1 Typ obiektu,

7.1.6.1.2 Kolor obiektu,

7.1.6.1.3 Rozmiar obiektu,

7.1.6.1.4 Prędkość obiektu.

7.1.6.1.5 Osoba

7.1.6.1.6 Zwierzę

7.1.6.1.7 Pojazd

7.1.6.2 Przechowywanie sklasyfikowanych obiektów w dedykowanej bazie danych śledzenia obiektów.

7.1.6.2.1 Wyświetlane są metadane dotyczące klasyfikacji obiektów.

Analityka detekcji ruchu

7.1.7 System powinien posiadać wbudowane algorytmy wizyjnej detekcji ruchu (VMD) i będzie w stanie wykonywać je na odbieranych strumieniach wideo.

7.1.8 System powinien oferować następujące opcje podstawowej i inteligentnej wizyjnej detekcji ruchu.

7.1.8.1 Podstawowa wizyjna detekcja ruchu

7.1.8.1.1 Podstawowy algorytm detekcji ruchu.

7.1.8.1.2 Podstawowe tłumienie zakłóceń.

7.1.8.2 Inteligentna wizyjna detekcja ruchu

7.1.8.2.1 Zaawansowane filtrowanie powtarzającego się ruchu, np. drzew lub trawy.

7.1.8.2.2 Śledzenie ładunków świetlnych.

7.1.8.2.3 Zaawansowane algorytmy detekcji ruchu przeznaczone dla scen zewnętrznych.

7.1.9 Wbudowana detekcja ruchu w wersji Basic i Smart powinna posiadać następujące cechy:

7.1.9.1 Zmienna czułość.

7.1.9.2 Maskowanie rozmiaru.
7.1.9.3 Odrzucanie obiektów mniejszych/większych niż określony rozmiar.
7.1.9.4 Wielostrefowe obszary VMD na kamerę z możliwością zmiany czułości w każdej strefie.
7.1.9.5 Możliwość ustawienia trybu dziennego/nocnego w celu włączenia różnych ustawień funkcji wizyjnych dla dnia i nocy.
7.1.9.6 Automatyczne przełączanie dzień/noc lub przełączanie o określonych porach ma być opcjonalne.
7.1.9.7 Harmonogram umożliwiający włączanie/wyłączanie wybranych wyzwalaczy zdarzeń VMD w określonych porach dnia.

7.1.10 W przypadku konfiguracji VMD system powinien umożliwiać użytkownikom podgląd obrazu bieżącego lub zarejestrowanego na potrzeby konfiguracji/testów VMD.

7.1.11 System powinien mieć możliwość pokazywania obszarów maskowania VMD, w tym:
7.1.11.1 Wyzwalacze VMD.
7.1.11.2 Obszary detekcji VMD.

Analityka podstawowa, pośrednia i zaawansowana

7.1.12 System powinien umożliwiać podstawową, pośrednią i zaawansowaną analitykę wideo.

7.1.13 System powinien umożliwiać wyzwalanie zdarzeń na podstawie wyzwalaczy generowanych przez podstawową, pośrednią i zaawansowaną analitykę.

7.1.14 System oferuje następujące opcje wyzwalania zdarzeń:
7.1.14.1 Analityka podstawowa.
7.1.14.2 Podstawowe wyzwalacze przekroczenia linii.
7.1.14.3 Podstawowe wyzwalacze obecności.
7.1.14.4 Analityka pośrednia.
7.1.14.5 Zaawansowane wyzwalacze przekroczenia linii.
7.1.14.6 Zaawansowane wyzwalacze obecności.
7.1.14.7 Zaawansowana analityka.
7.1.14.8 Zaawansowane wyzwalacze przekroczenia linii.
7.1.14.9 Zaawansowane wyzwalacze obecności.
7.1.14.10 Wykrywanie prędkości.
7.1.14.11 Filtry rozmiaru i kierunku.

Liczenie głów

7.1.15 System powinien zapewniać następujące algorytmy zliczania osób i opcje możliwości:
7.1.15.1 Śledzenie głów z góry; algorytm na standardowej kamerze kolorowej patrzącej prosto w dół oferuje wyzwalanie zdarzeń, gdy głowy przekroczą linię.
7.1.15.2 Skośny lokalizator głów; algorytm w standardowej kamerze kolorowej zamontowanej pod kątem oferuje wyzwalanie zdarzenia, gdy głowy przekroczą linię.

Algorytm długości kolejki

7.1.16 System powinien oferować wyzwalanie zdarzeń w przypadku przekroczenia przez kolejkę określonej długości.

Algorytm dla obiektów nieruchomych

7.1.17 System powinien oferować wyzwalanie zdarzenia, gdy obiekt został pozostawiony na pewien czas.

Wykrywanie sabotażu kamery

7.1.18 System powinien być standardowo wyposażony w wideoanalizę wykrywania sabotażu kamery.

7.1.18.1 Wykrywanie sabotażu kamery obejmuje:

7.1.18.1.1 zakrywanie obiektywu (np. malowanie sprayem)

7.1.18.1.2 Poruszanie kamerą,

7.1.18.1.3 zmianę/zdejmowanie/usuwanie ostrości z obiektywu.

7.1.19 System powinien umożliwiać dodanie do każdej skonfigurowanej kamery funkcji wykrywania sabotażu kamery.

7.1.20 System powinien umożliwiać wyzwalanie zdarzeń w przypadku sabotażu kamery.

7.1.21 System powinien wyświetlać powiadomienie o alarmie w interfejsie operatora w przypadku wykrycia sabotażu.

7.1.22 System eliminuje fałszywe alarmy, wymagając, aby sabotaż trwał 60 sekund, zanim zostanie uznany za prawdziwy.

7.1.23 System powinien ograniczać możliwość resetowania sabotażu kamery przez użytkownika na podstawie praw dostępu przyznanych przez administratora.

Baza danych ruchu

7.1.24 System powinien umożliwiać utworzenie bazy danych Motion Database, która gromadzi dane o ruchu z wybranych kamer.

7.1.24.1 System powinien umożliwiać wykorzystanie danych o ruchu z Motion Database do informowania funkcji Activity Trails i Motion Area Search interfejsu operatora w wybranych kamerach.

7.1.25 System powinien umożliwiać ustawienie różnych poziomów czułości śledzenia danych o ruchu; im wyższa czułość, tym dokładniej śledzony jest ruch.

7.1.26 System powinien umożliwiać ustawienie rozmiaru siatki, w której śledzone są dane o ruchu, za pomocą jednej z następujących metod:

7.1.26.1 Aspect Ratio and Granularity Settings (im drobniejsza ziarnistość, tym więcej ruchu jest wykrywane w mniejszych obszarach obrazu).

7.1.26.2 Ręczne ustawianie rozmiaru siatki.

8 Wyzwalacze, zdarzenia i działania

Możliwości ogólne

8.1.1 System powinien ograniczać dostęp do zarządzania zdarzeniami wyłącznie do administratorów.

8.1.2 System powinien umożliwiać generowanie zdarzeń systemowych na podstawie skonfigurowanych wyzwalaczy systemowych oraz wykonywanie skonfigurowanych działań związanych ze zdarzeniami.

8.1.3 System powinien umożliwiać automatyczne przechowywanie wszystkich zdarzeń systemowych w bazie danych zdarzeń systemowych, nawet jeśli ze zdarzeniem nie jest powiązane żadne wideo. Więcej informacji na ten temat znajduje się w rozdziale Bazy danych.

Wyzwalacze zdarzeń

8.1.4 System powinien mieć możliwość generowania zdarzeń z następujących wyzwalaczy:

8.1.4.1 Wyzwalacz z kamer/enkoderów w sieci. Obejmuje to wejścia fizyczne lub wyzwalacze analityki wizyjnej z kamer.

8.1.4.2 Własna detekcja i analiza ruchu w systemie.

8.1.4.3 Urządzenia innych firm (np. kontrola dostępu, centrale sygnalizacji pożaru, centrale alarmowe, punkty sprzedaży itp.)

8.1.4.4 Zdarzenia użytkownika lokalnego (zdarzenia inicjowane przez operatora).

8.1.4.5 Nagrania inicjowane przez harmonogram czasowy.

Konfiguracja zdarzeń

8.1.5 System powinien posiadać funkcję "AND", która zapobiega występowaniu wyzwalaczy, jeśli nie występuje wyzwalacz zdarzenia ORAZ wejście We/Wy.

8.1.6 System powinien umożliwiać przypisanie harmonogramów do zdarzenia, w czasie których zdarzenie jest uważane za ważne. Zdarzenie nie będzie aktywne w czasie poza godzinami określonymi w przypisanym harmonogramie.

8.1.7 System powinien umożliwiać ustawienie ograniczenia częstotliwości wyzwalania zdarzeń.

8.1.8 System powinien umożliwiać ustawienie, które odrzuca krótkie zdarzenia wyzwalające, w wyniku czego zdarzenia są wyzwalane tylko wtedy, gdy poziomy wyzwalania pozostają wysokie przez czas trwania (lub przekraczają) okres filtra.

8.1.9 System powinien zapewniać ustawienie "poziomu priorytetu" dla zdarzeń, które mają być wysyłane jako alarmy do interfejsu operatora lub bramy zarządzania alarmami.

Działania związane ze zdarzeniami

8.1.10 System powinien umożliwiać wykonanie jednego lub więcej z następujących działań po otrzymaniu sygnału wyzwalającego zdarzenie:

8.1.10.1 Wykonać działanie albo "podczas" występowania zdarzenia, albo "po" wystąpieniu zdarzenia.

8.1.10.2 Nagrywanie materiału wideo z jednej lub więcej kamer do wybranej bazy danych.
8.1.10.3 Zapisywanie zdarzeń wstępnych z jednej lub więcej kamer.
8.1.10.4 Nagrywanie zsynchronizowanego obrazu i dźwięku.
8.1.10.5 Przełączanie lub przełączanie jednego lub więcej wyjść przekaźnikowych, które są dostarczane przez system lub kamery/kodery podłączone do systemu.
8.1.10.6 "Impulsowanie" jednego lub więcej wyjść przekaźnikowych, które są dostarczane przez system lub kamery/kodery podłączone do systemu.
8.1.10.7 Sterowanie wirtualnym wejściem.
8.1.10.8 Przesunięcie jednej lub więcej kamer PTZ do pozycji "Preset".
8.1.10.9 Przełączanie jednej lub więcej wybranych kamer na jeden lub więcej wybranych monitorów podłączonych do systemu.
8.1.10.10 Przełączanie "układu" kamer na wybrany monitor.
8.1.10.11 Nagrywanie danych z systemów innych firm (np. punktów sprzedaży, kontroli dostępu, paneli alarmowych).
8.1.10.12 Inicjowanie akcji graficznej na mapie.
8.1.10.13 Odtwarzanie nagranego wcześniej klipu dźwiękowego za pośrednictwem lokalnego serwera klienckiego LUB za pośrednictwem wyjścia audio w kamerze IP lub nadajniku.
8.1.10.14 Wysyłanie wiadomości e-mail do wybranych odbiorców.
8.1.10.15 Wysyłanie alarmu do interfejsu operatora i bramy zarządzania alarmami (patrz Punkt 12).
8.1.10.15.1 Po wysłaniu powiadomienia do Bramy Alarmowej, system powinien umożliwiać użytkownikowi zdefiniowanie podglądu wideo, który ma być wysyłany wraz z powiadomieniem o zdarzeniu.
8.1.10.15.2 Zdarzenia skonfigurowane z "poziomami priorytetu" będą prezentowały użytkownikom alarmy o odpowiednich poziomach priorytetu.
8.1.10.16 Zatrzymanie wcześniej rozpoczętej akcji.
8.1.10.17 System powinien umożliwiać podporządkowanie wszystkich działań harmonogramom czasowym zdefiniowanym przez użytkownika.
8.1.10.18 System powinien umożliwiać tworzenie "szablonów zdarzeń", dzięki którym użytkownicy będą mogli w łatwy sposób powiązać wspólne działania dla wielu kamer.

9 Integracja

Możliwości ogólne

9.1.1 System powinien posiadać możliwość integracji produktów i urządzeń innych firm.

9.1.2 System nie powinien uruchamiać integracji firm trzecich jako wtyczek w kliencie oprogramowania.

9.1.3 System nie powinien wymagać dodatkowych serwerów zarządzających do uruchomienia usług integracyjnych innych firm.

9.1.4 System powinien centralizować wszystkie integracje do jednego punktu w oprogramowaniu.

9.1.5 System powinien umożliwiać konfigurację baz danych specyficznych dla każdej integracji, z wykorzystaniem sterowników specyficznych dla danej integracji. Więcej informacji na ten temat znajduje się w rozdziale Bazy danych.

9.1.6 System nie będzie już łączył się z urządzeniami integracyjnymi działającymi na obiektach z systemem CathexisVision 2017 i wcześniejszymi oraz nie będzie otrzymywał od nich statusów i powiadomień.

9.1.7 Możliwości integracji będą zależały od urządzenia zintegrowanego, ale system powinien mieć możliwość korzystania z następujących funkcji:

9.1.7.1 Odbiór danych z urządzenia innej firmy.

9.1.7.2 Pobieranie określonych wyzwalaczy zdarzeń i wykonywanie działań związanych ze zdarzeniami w zależności od otrzymanych określonych danych.

9.1.7.3 Przechowywanie danych w polach logicznych w wybranej bazie danych.

9.1.7.4 Skojarzenie jednej lub wielu kamer z obiektami urządzeń integracyjnych i związanymi z nimi zdarzeniami.

9.1.7.5 Wyświetlanie otrzymanych danych jako nakładki na skojarzone kamery w trybie podglądu na żywo i podglądu (tam gdzie to możliwe).

9.1.7.6 Wyświetlanie i konfiguracja właściwości urządzenia integracyjnego, takich jak:

9.1.7.6.1 Konfiguracja obiektów urządzenia integracyjnego.

9.1.7.6.2 Ustawianie i przeglądanie właściwości statusu obiektów urządzenia integracyjnego.

9.1.7.6.3 Wyświetlanie zdarzeń urządzenia integracyjnego.

9.1.7.6.4 Konfiguracja grup obiektów urządzenia integracyjnego.

9.1.7.6.5 Konfiguracja innych ustawień urządzenia integracyjnego, takich jak nakładki, timeouty, itp.

Lista urządzeń integracyjnych

9.1.8 System powinien umożliwiać integrację z różnymi produktami i urządzeniami firm trzecich, w tym (ale nie tylko) z następującymi:

9.1.8.1 Kontrola dostępu.

9.1.8.2 Punktami sprzedaży.

9.1.8.3 Panele alarmowe.

9.1.8.4 Centrale przeciwpożarowe.

9.1.8.5 Automatyczne rozpoznawanie tablic rejestracyjnych.

9.1.8.6 Monitorowanie ogrodzeń i obrzeży.

9.1.8.7 Monitorowanie środowiska.

9.1.8.8 Analityka wideo innych producentów.

9.1.8.9 Klawiatury i sterowniki.

9.1.9 System powinien być zintegrowany z urządzeniami we/wy w celu sterowania wyjściami i odbierania sygnałów wejściowych z urządzeń we/wy. Urządzenia te mogą znajdować się w kamerze sieciowej, koderze (serwerze) lub w dedykowanym sieciowym urządzeniu We/Wy.

10 Automatyczne rozpoznawanie tablic rejestracyjnych (Automatic Number Plate Recognition - ANPR)

Ogólne funkcje

10.1.1 System powinien obejmować automatyczne rozpoznawanie tablic rejestracyjnych jako funkcję opcjonalną.

10.1.2 System powinien integrować się z trzema kategoriami silników ANPR:

10.1.2.1 Algorytmy ANPR innych firm, które wysyłają sygnały wyzwalające ANPR do systemu CathexisVision;

10.1.2.2 Kamery ANPR z wbudowaną funkcją wykrywania ANPR, które wysyłają sygnały wyzwalające do VMS; oraz

10.1.2.3 Silniki ANPR, które są wbudowane w system VMS i które są odblokowane za pomocą odpowiednich licencji.

10.1.3 Wbudowany system powinien posiadać następujące możliwości:

10.1.3.1 Obsługa wielu bibliotek języków i znaków tablic rejestracyjnych, w tym arabskich.

10.1.3.2 Obsługuje konfigurację wykrywania tablic rejestracyjnych dla następujących rozwiązań w zakresie wykrywania:

10.1.3.2.1 Rozwiązanie wyzwalane, które wykorzystuje fizyczne wyzwalanie do zainicjowania detekcji (takie jak pętla uziemienia, wiązka IR lub rozwiązanie VMD), oraz.

10.1.3.2.2 Rozwiązanie swobodnego przepływu, które wykrywa tablice rejestracyjne poruszających się pojazdów.

10.1.3.3 System powinien umożliwiać nakładanie danych o wykrytych tablicach rejestracyjnych na strumienie obrazu bieżącego i zapisanego.

10.1.4 System powinien posiadać możliwość importu/eksportu istniejących danych ANPR w formacie pliku CSV.

Wbudowane w system detektory ANPR

10.1.5 System powinien umożliwiać konfigurowanie wielu detektorów ANPR w ramach interfejsu ustawień w już zainstalowanych kamerach, pod warunkiem dostępności wymaganych licencji.

10.1.6 System powinien obsługiwać następujące opcje detektorów:

10.1.6.1 Konfiguracja specyficzna dla kamery, taka jak rozdzielczość i liczba klatek na sekundę.

10.1.6.2 Wybór obszaru przechwytywania tablicy rejestracyjnej pojazdu.

10.1.6.3 Konfiguracja rozmiaru, nachylenia i pochylenia znaków tablicy rejestracyjnej.

10.1.6.4 Konfiguracja analizy tablicy rejestracyjnej w oparciu o wyzwalacz wejściowy, taki jak pętla uziemienia lub ruch.

10.1.6.5 Testowanie (analiza tablic rejestracyjnych) konfiguracji ANPR z wykorzystaniem zarejestrowanego materiału filmowego z miejsca zdarzenia w celu dokładnego dostrojenia algorytmu.

Zasady ANPR

10.1.7 System powinien umożliwiać grupowanie danych dotyczących tablic rejestracyjnych w określone kategorie, takie jak goście, personel, biała lista, czarna lista itp.

10.1.8 System powinien umożliwiać skonfigurowanie następujących reguł analizy ruchu, które generują komunikaty systemowe w przypadku wykrycia określonych wzorców ruchu:

10.1.8.1 Reguła lokalizacji wizyty uruchamia się, gdy tablica rejestracyjna jest widziana w tej samej lokalizacji wielokrotnie.

10.1.8.2 Reguła dotycząca odwiedzanego obszaru uruchamia się, jeżeli tablica rejestracyjna jest widziana w wielu miejscach w danym okresie czasu.

Zdarzenia ANPR

10.1.9 System powinien umożliwiać tworzenie zdarzeń wyzwalanych za pomocą rozpoznawania tablic rejestracyjnych.

10.1.10 System powinien umożliwiać konfigurowanie zdarzeń na podstawie danych dotyczących konkretnej tablicy rejestracyjnej i zdarzenia.

10.1.11 System powinien umożliwiać konfigurowanie zdarzeń w oparciu o dane dotyczące grup tablic rejestracyjnych.

10.1.12 System powinien umożliwiać wyzwalanie działań związanych ze zdarzeniami, które obejmują, lecz nie ograniczają się do wyzwalania urządzeń we/wy w celu kontroli dostępu.

10.1.13 System powinien umożliwiać generowanie raportów o zdarzeniach ANPR:

10.1.13.1 Raporty o zdarzeniach powinny być eksportowane w formacie pliku PDF lub CSV.

10.1.13.2 Raporty ze zdarzeń generowane są w oparciu o filtry danych dotyczące danych ANPR pojazdu.

10.1.13.3 Raporty o zdarzeniach generowane są na podstawie określonych przedziałów czasowych.

Alarmy ANPR

10.1.14 System powinien umożliwiać generowanie alarmów na podstawie zdarzeń ANPR, takich jak:

10.1.14.1 Dane o zdarzeniach ANPR pojawiające się na czarnej liście danych tworzą alarm.

10.1.14.2 Dane o zdarzeniach ANPR dotyczące tego samego pojazdu, zarejestrowane wielokrotnie w określonym czasie, powodują uruchomienie alarmu.

10.1.14.3 Dane o zdarzeniach ANPR dotyczące tego samego pojazdu zarejestrowanego wielokrotnie w wielu strefach w określonym czasie powodują uruchomienie alarmu.

11 Brama zarządzania alarmami

Funkcje ogólne

11.1.1 System zapewnia funkcję zarządzania alarmami umożliwiającą zgłaszanie alarmów wywołanych przez lokalny i zdalny system oraz zarządzanie nimi.

11.1.2 System powinien umożliwiać podłączenie do urządzenia AMG za pomocą interfejsu operatora.

11.1.3 System powinien umożliwiać połączenie systemów za pomocą protokołu TCP/IP, poprzez sieci LAN/WAN.

11.1.4 Systemowe rozwiązanie pomieszczenia kontrolnego powinno umożliwiać dwukierunkową transmisję dźwięku i monitorowanie.

11.1.5 System zarządzania alarmami powinien w określonych odstępach czasu monitorować połączenia z jednostkami zdalnymi za pomocą sygnalizatora pracy obiektu. Generuje on sygnał wyzwalający, gdy zdalna jednostka alarmowa nie wysyła sygnałów sercowych.

11.1.6 Z systemu zarządzania alarmami powinna istnieć możliwość wysyłania SMS-ów z alarmami technicznymi i alarmami o zdarzeniach.

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

Interfejs AMG

11.1.8 System powinien umożliwiać operatorom dyspozytorni korzystanie z interfejsów wielomonitorowych, z pulpitami alarmów, zasobów, map i innego oprogramowania rozmieszczonego na monitorach.

11.1.9 Interfejs alarmowy systemu powinien posiadać wyraźnie widoczny graficzny wskaźnik stanu połączenia z bramą (połączona lub rozłączona). System jest opcjonalnie skonfigurowany w taki sposób, aby po nawiązaniu połączenia operator widział pulpit/konfigurację ekranu dostosowaną do potrzeb klienta, informacje o alarmie oraz mapę dotyczącą tego konkretnego alarmu.

11.1.10 System powinien umożliwiać konfigurację mapy w taki sposób, aby ikona alarmu o zdarzeniu migała w odpowiednim miejscu, w którym alarm został zainicjowany.

11.1.11 System wyświetla alarmy w oddzielnych panelach w zależności od stanu:
11.1.11.1 Przychodzące (oczekujące na obsługę przez operatora).
11.1.11.2 Bieżący (obsługiwany przez operatora).
11.1.11.3 Zarchiwizowany (już obsługiwany przez operatora).

11.1.12 System powinien umożliwiać dostosowanie dźwiękowych powiadomień o alarmie przychodzącym.

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

11.1.14 W kolejce alarmów przychodzących, które nie zostały obsłużone, system emituje dźwięk powiadomienia dźwiękowego o alarmie o najwyższym priorytecie przez 30 sekund do momentu obsłużenia.

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

11.1.16 Nawet po przejściu z pulpitu kolejki alarmowej system powinien wyświetlać pasek stanu alarmu wskazujący liczbę przychodzących, nie obsłużonych alarmów według priorytetu oznaczonego kolorem.

Działania operatora

11.1.17 System powinien umożliwiać operatorom reagowanie na alarm i automatyczne łączenie się z miejscem, z którego alarm został zainicjowany.

11.1.18 System powinien umożliwiać czasowe wyłączenie (zablokowanie) powtarzających się nieważnych alarmów na określony czas. Blokada ta jest określana z poziomu jednostki bramowej i wymaga wyjaśnień ze strony operatora blokującego.

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

11.1.20 System powinien umożliwiać operatorom jednoczesną obsługę wielu alarmów zdalnych - każde połączenie powinno być reprezentowane przez oddzielną kartę interfejsu.

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

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

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

11.1.24 System powiadamia użytkowników, którym przydzielono sprawy, o przydzielonych im zadaniach.

11.1.25 System powinien umożliwiać operatorom utworzenie sprawy niezależnie od alarmu.

11.1.26 System powinien zapewniać narzędzie do zarządzania sprawami, umożliwiające elektroniczną współpracę pomiędzy wszystkimi przydzielonymi stronami, zaangażowanie ważnych pracowników w proces oraz zapewnienie, że sprawa musi być odpowiednio rozwiązana/podpisana zanim zostanie "zamknięta".

11.1.27 System powinien pozwalać kierownikom spraw na dalszą eskalację spraw na wyższe poziomy kontroli.

11.1.28 System powinien umożliwiać operatorom filtrowanie alarmów historycznych z wykorzystaniem powiązanych z nimi nagrań i metadanych. Parametry filtrowania powinny obejmować:

11.1.28.1 Alarmy, Sesje (gdzie wiele alarmów mogło zostać wysłanych przez jedno połączenie).
11.1.28.2 Operator sterowni (na podstawie informacji o logowaniu).
11.1.28.3 Przypadki (alarmy, które zostały eskalowane do dalszego badania).

11.1.29 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 powinny być możliwe następujące czynności:
11.1.29.1 Wyświetlenie nazwy miejsca alarmowania.
11.1.29.2 Wyświetlenie nazwy serwera alarmowego.
11.1.29.3 Wyświetlenie opisu alarmu.
11.1.29.4 Wyświetlanie operatora sterowni, który obsługiwał alarm lub sesję.
11.1.29.5 Wyświetlenie nazwy jednostki dyspozytorskiej, przez którą obsługiwany był alarm lub sesja.
11.1.29.6 Wyświetlenie czasu wystąpienia zdarzenia alarmowego.
11.1.29.7 Wyświetlenie czasu, w którym zdarzenie alarmowe zostało wysłane do dyspozytorni.
11.1.29.8 Wyświetlenie czasu dotarcia alarmu do dyspozytorni.
11.1.29.9 Podgląd czasu potrzebnego na obsłużenie alarmu przez Operatora dyspozytorni.
11.1.29.10 Przeglądanie komentarzy związanych z alarmami, sesjami i sprawami.
11.1.29.11 "Dodaj komentarz i zamknij alarm" przy dodawaniu komentarza z okna odtwarzania obrazu alarmu. Po dodaniu komentarza alarm zostanie zamknięty.
11.1.29.12 Przeglądanie nagrań powiązanych z alarmem.
11.1.29.13 Nawiązanie połączenia z historyczną lokalizacją alarmowania w celu pobrania dalszych nagrań związanych z alarmem, jeśli istnieją one w bazie danych lokalizacji zdalnej.
11.1.29.14 Przeglądanie spraw związanych z alarmem.
11.1.29.15 Wyświetlanie całej Sesji, w której obsługiwany był alarm.
11.1.29.16 Dodawanie dalszych komentarzy do historycznych alarmów, sesji i przypadków.
11.1.29.17 Eskalacja alarmu historycznego do Sprawy w celu dalszego zbadania i rozwiązania.
11.1.29.18 Wyświetlanie loginów Operatorów z dyspozytorni związanych z sesją alarmową.
11.1.29.19 Wyświetlanie wszystkich alarmów powiązanych z sesją.
11.1.29.20 Wyświetlenie czasu trwania, godziny rozpoczęcia i zakończenia logowania Operatora Dyspozytorni.
11.1.29.21 Przeglądanie liczby Sesji obsługiwanych przez Operatora w trakcie Logowania.
11.1.29.22 Wyświetlenie wszystkich Sesji obsługiwanych przez Operatora w trakcie Logowania.
11.1.29.23 Wyświetlenie opisu sprawy.
11.1.29.24 Wyświetlenie nazwy użytkownika, który eskalował alarm do Sprawy, wraz z datą i godziną.
11.1.29.25 Wyświetlenie nazwy użytkownika, który zamknął Sprawę, wraz z datą i godziną.
11.1.29.26 Wyświetlenie listy użytkowników Sprawy, wraz z ich Statusem odnoszącym się do Sprawy (Aktywny - nadal nad nią pracuje lub Nieaktywny - już nad nią nie pracuje).
11.1.29.27 Wyświetlanie osi czasu działań użytkownika związanych z daną Sprawą.
11.1.29.28 Przeglądanie Statusu Sprawy.
11.1.29.29 Przeglądanie wszystkich Alarmów powiązanych ze Sprawą.
11.1.29.30 Wyświetlanie wszystkich komentarzy powiązanych ze Sprawą.

Raportowanie AMG

11.1.30 System powinien zapewniać szczegółowe, konfigurowalne raporty oparte na połączeniach, czasach odpowiedzi, logowaniach i czasach obsługi.

11.1.31 System powinien tworzyć ścieżkę audytu i harmonogram odpowiedzi na zgłoszenia.

11.1.32 System rejestruje logowania operatora i odpowiedzi na połączenia przychodzące oraz chroni te informacje przed manipulacją.

11.1.33 System powinien być zdolny do zaplanowania automatycznego uruchamiania raportów oraz do wykonywania automatycznych działań z raportami, takich jak wysyłanie raportów pocztą elektroniczną do odbiorców.

12 Klawiatura zintegrowana

Natywna klawiatura/sterownik

12.1.1 System powinien być wyposażony w zintegrowaną klawiaturę sterującą.

12.1.2 System powinien umożliwiać konfigurację czułości obrotu/pochylenia/powiększenia w oprogramowaniu.

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

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

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

12.1.6 Diody LED na klawiszach klawiatury powinny wskazywać stan klawiszy i funkcji.

Klawiatura/sterownik innej firmy

12.1.7 System powinien umożliwiać integrację klawiatur i kontrolerów innych producentów.

13 Bazy danych

Zdolności ogólne

13.1.1 System powinien zapewniać szybki i łatwy dostęp do wszystkich baz danych z poziomu interfejsu operatora.

13.1.2 System powinien umożliwiać konfigurację wielu baz danych oraz kierowanie wielu kamer i/lub grup kamer do jednej lub więcej baz danych.

13.1.3 System powinien ograniczać przeglądanie wpisów w bazie danych, pozwalając użytkownikom z odpowiednimi prawami dostępu do podglądu kamer na przeglądanie określonych kamer w bazie danych.

Baza danych wideo

13.1.4 System powinien zapewniać własną bazę danych wideo, która nie jest zależna od silników baz danych innych firm (takich jak PostgreSQL i MySQL).

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

13.1.6 System powinien kontynuować zapis do bazy danych nawet w przypadku awarii jednego/wielu dysków.

13.1.7 System obsługuje następujące cechy baz danych:

13.1.7.1 Zmienny rozmiar dysków

13.1.7.2 Rozłożenie obciążenia zapisem na wiele dysków.

13.1.7.3 Bazy danych można eksportować i przenosić z jednego urządzenia NVR do drugiego.

13.1.7.4 Rozbudowa istniejącej bazy danych poprzez dodanie większej przestrzeni dyskowej.

13.1.7.5 Zapewnienie możliwości odzyskania danych w przypadku uszkodzenia systemu plików przy minimalnej utracie danych.

13.1.8 System powinien umożliwiać przeglądanie wpisów w bazie danych w zależności od wyboru daty i znacznika czasu.

13.1.9 System powinien umożliwiać skonfigurowanie maksymalnego okresu zapisu.

Baza danych metadanych (integracyjnych)

13.1.10 System powinien umożliwiać tworzenie dedykowanych baz danych integracyjnych dla każdej integracji. Bazy danych integracji powinny:

13.1.10.1 Posiadać zintegrowany odtwarzacz wideo.

13.1.10.2 Łączyć dane z urządzeń zintegrowanych z danymi wideo pobranymi z kamer towarzyszących.

13.1.10.3 Odtwarzać wideo i dane jednocześnie i synchronicznie w odtwarzaczu wideo zintegrowanej bazy danych.

13.1.10.4 Wyświetlanie wszystkich kamer powiązanych ze zdarzeniami urządzenia.

13.1.10.5 Wykonywanie "łatwego wyszukiwania" za pomocą rozwijanego interfejsu użytkownika, który natychmiast filtruje wpisy zgodnie z dostępnymi opcjami łatwego wyszukiwania (unikalnymi dla każdej integracji).

13.1.10.6 Zapewnienie możliwości "kopania" bazy danych w celu znalezienia wybranych danych/transakcji oraz powiązanych danych wideo, przy użyciu filtrów właściwych dla danej integracji oraz opcji przeglądania/wyszukiwania/sortowania.
13.1.10.7 Umożliwienie eksportu wpisów do bazy danych w formacie PDF i CSV.
13.1.10.8 Potrafi archiwizować video i powiązane meta-dane z odtwarzacza video bazy danych integracji.
13.1.10.9 Możliwośd tworzenia zaplanowanych raportów meta bazy danych.
13.1.10.10 Możliwośd rozszerzonego filtrowania raportów

Baza danych zdarzeń systemowych

13.1.11 System powinien umożliwiać tworzenie bazy danych zdarzeń, do której wszystkie zdarzenia systemowe są kierowane automatycznie, bez konieczności konfigurowania akcji rejestrowania zdarzeń.

Integracyjna baza danych ANPR

13.1.12 System powinien umożliwiać utworzenie specyficznej dla zdarzenia integracyjnej bazy danych ANPR.

13.1.13 System powinien umożliwiać przeglądanie, sortowanie i "łatwe przeszukiwanie" bazy danych ANPR według następujących kryteriów:
13.1.13.1 Tablice rejestracyjne.
13.1.13.2 Grupy tablic rejestracyjnych.
13.1.13.3 Detektory ANPR/LPR.

13.1.14 System powinien umożliwiać filtrowanie bazy danych ANPR według szeregu opcji, w tym między innymi według następujących kryteriów:
13.1.14.1 Czas/Data.
13.1.14.2 Tablice rejestracyjne/grupy
13.1.14.3 Zaufanie (dokładność wychwytywania tablic rejestracyjnych w procentach).
13.1.14.4 Detektor ANPR.
13.1.14.5 Kamera.
13.1.14.6 Nazwisko kierowcy/firmy.
13.1.14.7 Typ/marka/model/kolor pojazdu.
13.1.14.8 Miejsce wydania (w zależności od regionu)
13.1.14.9 Kolor tła, kolor tekstu i kształt tablicy rejestracyjnej.
13.1.14.10 Umiejscowienie tablicy rejestracyjnej na samochodzie (przód/tył).
13.1.14.11 Położenie pojazdu na pasie ruchu (wjazd/wyjazd).

Baza danych klasyfikacji obiektów

13.1.15 System powinien umożliwiać tworzenie integracyjnej bazy danych do przechowywania zarejestrowanego obrazu związanego ze śledzeniem i klasyfikacją obiektów.

13.1.16 Poza posiadaniem wszystkich cech integracyjnej bazy danych (pkt 13.3), baza danych śledzenia obiektów powinna dostarczać metadane o klasyfikowanym obiekcie, które mogą być wyświetlane w nakładkach.

13.1.17 Metadane klasyfikacji obiektów obejmują:

13.1.17.1 Klasyfikację obiektu, która została dokonana.
13.1.17.2 Poziom ufności klasyfikacji.
13.1.17.3 Kolor i kolor zastępczy obiektu.
13.1.17.4 Czas rozpoczęcia i zakończenia klasyfikacji.
13.1.17.5 Wielkość (szerokość i wysokość w cm) obiektu.
13.1.17.6 Prędkość obiektu.

14 Failover

Zdolności ogólne

14.1.1 System powinien umożliwiać Failover serwerów n:1 i n:n.

14.1.1.1 Serwer awaryjny może przejąć funkcje dowolnego serwera, który uległ awarii.

14.1.1.2 Do realizacji tego celu będzie wykorzystywana struktura hotspare.

14.1.2 System powinien być zdolny do awaryjnego przejęcia serwera głównego/zarządzającego i wszystkich związanych z nim funkcji, w tym między innymi:

14.1.2.1 Nagrywanie i przeglądanie wideo.

14.1.2.2 Podgląd obrazu na żywo, w tym funkcje sterowania ścianą wizyjną.

14.1.2.3 Konfiguracja zdarzeń i zarządzanie nimi.

14.1.3 System powinien zapewniać możliwość prostej konfiguracji awaryjnej podczas procesu instalacji oprogramowania VMS.

14.1.4 System powinien zapewniać bazę danych awaryjnych, która rezyduje na samym serwerze awaryjnym

Proces przejmowania funkcji w przypadku awarii

14.1.5 Serwer awaryjny będzie w sposób ciągły monitorował serwery zarządzania i rejestracji.

14.1.6 Serwer awaryjny przejmuje funkcjonalność serwera, który uległ awarii, umożliwiając kontynuację działania obiektu.

14.1.7 System automatycznie ponownie umieszcza obraz wideo w bazie danych pierwotnego serwera nagrywającego po odzyskaniu uszkodzonego serwera.

14.1.8 System powinien generować alarm w przypadku awarii serwera w miejscu instalacji i jego przełączenia.

14.1.9 System powinien generować alarm w przypadku awarii serwera awaryjnego.

14.1.10 System powinien udostępniać funkcję Site Overview, która wyświetla wszystkie serwery lokalne ze wskazaniem serwera, który uległ awarii.

15 Stan systemu

Raporty techniczne

15.1.1 System powinien oferować rozbudowane raporty dotyczące sprzętu i oprogramowania wchodzącego w skład witryny poprzez prowadzenie dzienników technicznych i umożliwienie generowania raportów technicznych.

15.1.2 System powinien ograniczać dostęp do konfiguracji raportów technicznych wyłącznie do administratorów.

15.1.3 System powinien umożliwiać użytkownikom zapisywanie swoich raportów jako "szablonów" w celu łatwego generowania przyszłych raportów.

15.1.4 System powinien pozwalać użytkownikom na eksport raportów w skompresowanym formacie html.

15.1.4.1 W formacie html system powinien umożliwiać automatyczne generowanie spisu treści oraz hiperłączy do sekcji.

15.1.5 System powinien umożliwiać wysyłanie raportów pocztą elektroniczną, drukowanie i archiwizowanie (zapisywanie).

15.1.6 System powinien umożliwiać automatyczne opracowywanie i wysyłanie pocztą elektroniczną wybranych raportów do wybranych odbiorców zgodnie z określonym harmonogramem.

15.1.7 System powinien umożliwiać generowanie raportów technicznych specyficznych dla serwera/sprzętu, dotyczących następujących zagadnień:

15.1.7.1 Awarie kamer, logi, status i czas do naprawy.

15.1.7.2 Użytkowania bazy danych:

15.1.7.2.1 Podział według kamer.

15.1.7.2.2 Stawka według kamery/godzinę/kamerę na godzinę.

15.1.7.2.3 Histogram częstotliwości zdarzeń.

15.1.7.2.4 Zdarzenia na godzinę.

15.1.7.3 Dysk.

15.1.7.4 Środowisko.

15.1.7.5 Zdarzenia.

15.1.7.6 Systemy plików.

15.1.7.7 Sprzęt.

15.1.7.8 Cechy licencji.

15.1.7.9 Licencje.

15.1.7.10 Zapytania NTP.

15.1.7.11 Ponowne uruchomienia i przyczyny ponownych uruchomień, w tym:

15.1.7.12 Restarty serwera oprogramowania.

15.1.7.13 Ponowne uruchomienia w przypadku awarii zasilania.

15.1.7.14 Ponowne uruchomienia użytkownika.

15.1.7.15 Ponowne uruchamianie użytkowników zdalnych.

15.1.7.16 Czas ponownego uruchomienia.

15.1.7.17 Ustawienia i konfiguracja zapisu, czasy (systemu na kamerę) oraz awarie zapisu.

15.1.7.18 Ustawienia i konfiguracja systemu.

15.1.7.19 Awarie serwera oprogramowania.
15.1.7.20 Czas pracy urządzenia.
15.1.7.21 VMX:
15.1.7.21.1 Liczniki.
15.1.7.21.2 Temperatury.
15.1.7.21.3 Alerty zdrowotne na pasku stanu. Komunikat będzie wyświetlany, jeśli dysk, na którym zainstalowany jest NVR, zapełni się.

Alarmy techniczne

15.1.8 System powinien umożliwiać generowanie alarmów technicznych specyficznych dla serwera/sprzętu, w tym między innymi:
15.1.8.1 Alarmy awarii Heartbeat.
15.1.8.2 Usterki kamery, jeżeli:
15.1.8.2.1 Np. Kamery uległy awarii więcej niż określoną liczbę razy w określonym przedziale czasu.
15.1.8.2.2 Np. kamery były wyłączone przez więcej niż określony procent czasu w określonym okresie.
15.1.8.3 Alarmy bazy danych (generowane, gdy zdarzenie jest wyzwalane, ale nie jest odbierany obraz wideo).
15.1.8.4 Alarmy dyskowe.
15.1.8.4.1 Np. parametry SMART dysku twardego poza normami wymaganymi przez system.
15.1.8.5 Alarmy środowiskowe (zależne od serwera/sprzętu)..
15.1.8.5.1 Np. temperatura, prędkość wentylatora.
15.1.8.6 Alarmy awarii.
15.1.8.7 Przełączenie serwera.
15.1.8.8 Awaria serwera awaryjnego.
15.1.8.9 Alarmy integracyjnej bazy danych.
15.1.8.10 Alarmy we/wy sieci.
15.1.8.11 Alarmy łączności sieciowej.
15.1.8.11.1 Np. w przypadku awarii medium komunikacyjnego, takiego jak Ethernet lub Modem.
15.1.8.11.2 Np. jeśli nie powiodło się automatyczne, rutynowe pingowanie stacji przechwytującej przez Alarm Management Gateway.
15.1.8.12 Alarmy restartu, Np. jeśli częstotliwość restartu jest nietypowo wysoka.
15.1.8.13 Alarmy okresu zapisu/awarii.
15.1.8.13.1 Np. jeśli liczba zarejestrowanych zdarzeń w danym dniu jest mniejsza niż powinna być (na podstawie średniej historycznej), co wskazuje na możliwą usterkę techniczną.
15.1.8.14 Zaplanowany alarm archiwalny.
15.1.8.15 Alarm monitorowania serwera.
15.1.8.15.1 Np. w przypadku wystąpienia nietypowej sekwencji wyłączenia (np. wyciągnięcie przez użytkownika przewodu zasilającego).
15.1.8.15.2 Np. Wszystkie systemy powinny w sposób ciągły testować wszystkie inne systemy w obiekcie pod kątem "up-time" i jeżeli któryś z systemów nie odpowiada, może zostać wysłany alarm.
15.1.8.16 Alarm awarii oprogramowania.
15.1.8.17 Alarm testowy.

15.1.8.18 Powinna istnieć możliwość uruchomienia próbnego alarmu technicznego z pojedynczej jednostki w obrębie stanowiska jednostek.

15.1.8.19 Wysyłanie alarmów powinno posiadać filtry umożliwiające użytkownikom ograniczenie liczby wysyłanych alarmów. Ustawienia te powinny obejmować:

15.1.8.19.1 Wysyłanie alarmu za każdym razem, gdy wystąpi zdarzenie.

15.1.8.19.2 Wysyłanie alarmu natychmiast, a następnie co określony okres czasu.

15.1.8.19.3 Wysyłanie alarmu tylko raz.

16 Dzienniki audytu

Możliwości ogólne

16.1.1 System powinien umożliwiać audyt witryn i serwerów, zapewniając historyczny dziennik wszystkich działań wykonywanych przez użytkowników.

16.1.2 System ogranicza dostęp do audytowanych witryn i serwerów wyłącznie do administratorów.

16.1.3 System powinien umożliwiać filtrowanie logów audytowych według następujących kryteriów:

16.1.3.1 Czas/Okres czasu.

16.1.3.2 Użytkownicy

16.1.3.3 Zasoby

16.1.3.4 Działania użytkownika

16.1.4 System powinien umożliwiać wyświetlanie dzienników audytowych filtrowanych według użytkowników, w celu wyświetlenia historycznego dziennika działań operatora, dla wszystkich loginów użytkowników.

16.1.5 System powinien umożliwiać eksport logów audytowych w formacie pliku CSV.

17 Narzędzie kryminalistyczne

Możliwości ogólne

17.1.1 System powinien posiadać narzędzie do analizy śledczej, które umożliwia analizę i rozwiązywanie problemów w miejscu instalacji w celu uzyskania następujących historycznych danych z serwera:

17.1.1.1 Podsumowanie kamer sieciowych - całkowita przepustowość sieci, współczynnik zrzutów i liczba zacięć kamer.

17.1.1.2 Zapisy bazy danych - bitrate zapisu na dysku oraz zrzuty do lokalnego lub sieciowego magazynu.

17.1.1.3 Zrzucone pakiety - sieć zewnętrzna, wewnętrzne UDP pomiędzy serwerami oraz wewnętrzne ramki wideo.

17.1.1.4 Strumieniowanie wideo - wysyłane, odbierane i dekodowane do podglądu na żywo.

17.1.1.5 Kompresor programowy - ilość zakodowanych i zdekodowanych pikseli oraz procent klatek.

17.1.1.6 Wewnętrzna wymiana komunikatów - pakiety UDP wysyłane i odbierane pomiędzy procesami oraz liczba wysyłanych logów na minutę.

17.1.1.7 Ramki wideo - nieodebrane i odebrane pomiędzy procesami wewnętrznymi.

17.1.1.8 System powinien być wyposażony w narzędzie kryminalistyczne do rozwiązywania problemów i uzyskiwania następujących danych historycznych specyficznych dla kamery:

17.1.1.9 Kamery sieciowe - bitrate, porzucone pakiety, zacięcia kamer, wyłączenia kamer oraz liczba zdarzeń na kamerę.

17.1.1.10 Kamery baz danych - bitrate, bajty zapisane na dysku, awaria kamery oraz liczba zdarzeń na kamerę.

17.1.2 System powinien umożliwiać prezentację danych kryminalistycznych w formie graficznej w oparciu o następujące elementy:

17.1.2.1 Wybór daty i godziny.

17.1.2.2 Wybór przedziału czasowego.

17.1.2.3 System powinien mieć możliwość ułatwienia następujących czynności w oknie wykresu:

17.1.2.4 Powiększanie przedziału czasowego danych.

17.1.2.5 Przeglądanie wartości danych.

17.1.2.6 Eksportowanie danych jako plik CSV.

18 Cyberbezpieczeństwo

Zdolności ogólne

18.1.1 W systemie powinny być stosowane środki bezpieczeństwa sprzętowego, programowego i cyberbezpieczeństwa w celu ograniczenia ryzyka dostępu do informacji i manipulacji danymi.

18.1.1.1 Środki te powinny być stosowane przez VMS równolegle do standardowych procedur bezpieczeństwa IT, w tym:

18.1.1.1.1 Właściwe kontrolowanie dostępu do sieci za pomocą takich technik jak:

18.1.1.1.1.1 Wdrażanie zapór ogniowych.

18.1.1.1.1.2 Stosowanie inteligentnych przełączników sieciowych.

18.1.1.1.1.3 Zarządzanie i kontrola "fizycznego" dostępu do sieci.

18.1.1.1.2 Zapobieganie nieautoryzowanemu dostępowi do systemu operacyjnego za pomocą takich technik jak:

18.1.1.1.2.1 Zapobieganie otwieraniu nieautoryzowanych portów umożliwiających korzystanie z elementów takich jak ftp, telnet, email, itp. Jeśli komunikacja musi odbywać się za pomocą tych środków, należy zapewnić stosowanie protokołów bezpieczeństwa, takich jak SSH/SFTP.

18.1.1.1.2.2 Wyłączenie dostępu "root" do systemu operacyjnego.

18.1.1.1.2.3 Zapewnienie poziomów silnych haseł.

18.1.1.1.2.4 Dodanie oprogramowania antywirusowego i anty-malware (z możliwością częstej aktualizacji).

18.1.1.1.2.5 Ograniczenie dostępu do Internetu.

Bezpieczna komunikacja pomiędzy komponentami VMS

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

18.1.2.1 Serwery nagrywające do klientów.

18.1.2.2 Serwery nagrywające do innych serwerów nagrywających.

18.1.2.3 Serwery nagrywające do Ścian Wizyjnych.

18.1.2.4 Serwery zapisu do bramy zarządzania alarmami.

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

18.1.3.1 Silnik szyfrujący powinien wykorzystywać szyfry symetryczne openssl (SHA512 hashes, ephemeral DH-RSA with forward secrecy [DH 2048 bit] oraz AES-GCM 128-bit) równoważne TLS 1.3.

18.1.3.2 Hasła nigdy nie są przechowywane jako zwykły tekst, lecz są haszowane za pomocą SHA512.

18.1.3.3 Dane uwierzytelniające do logowania są negocjowane przy użyciu RSA1024.

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

18.1.3.5 Do weryfikacji integralności wykorzystywany jest HMAC.

18.1.3.6 Wszystkie połączenia ze stronami zewnętrznymi obsługują różne poziomy szyfrowania:

18.1.3.6.1 Wyłączone.

18.1.3.6.2 Minimalny - szyfrowane są tylko połączenia krytyczne.

18.1.3.6.3 Secure (domyślnie) - szyfrowane są wszystkie połączenia z wyjątkiem połączeń z wideo o dużej objętości.

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

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

Bezpieczeństwo wizyjne

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

18.1.4.1 Podwójne klucze RSA1024 (do podpisywania) są używane w celu zabezpieczenia integralności eksportowanego/archiwizowanego obrazu.

18.1.4.2 Opcjonalne szyfrowanie wykorzystuje szyfrowanie blokowe AES128 z losowym IV na blok i hasłem generowanym przez użytkownika.

18.1.4.3 Filmy wideo mogą być znakowane znakiem wodnym w celu wskazania źródła informacji (tj. informacji o użytkowniku).

18.1.4.4 Materiał wideo i metadane ograniczone do odtwarzania za pomocą własnego odtwarzacza wideo VMS.

18.1.4.5 Odtwarzanie wyeksportowanych/archiwizowanych materiałów wideo może być ograniczone do odtwarzania kontrolowanego hasłem.

Zabezpieczenie kamer IP

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

18.1.5.1 Bezpieczne połączenie kamer:

18.1.5.1.1 HTTP: hipertekstowy protokół transferu.

18.1.5.1.2 Szyfrowane połączenia sterujące HTTPS.

18.1.5.1.3 Szyfrowane połączenia SSL/TLS.

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

18.1.5.2 Bezpieczne sterowanie kamerą:

18.1.5.2.1 RTSP - protokół strumieniowania w czasie rzeczywistym.

18.1.5.2.2 Sterowanie szyfrowane HTTPS.

18.1.5.3 Bezpieczna transmisja strumieniowa wideo:

18.1.5.3.1 RTP - protokół sterowania transportem w czasie rzeczywistym.

18.1.5.3.2 Zaszyfrowane wideo.

19 Edytor map

Oprogramowanie edytora map

19.1.1 Możliwości ogólne

19.1.1.1 System powinien automatycznie instalować wielowarstwową interaktywną mapę po zainstalowaniu oprogramowania serwera/klienta VMS.

19.1.1.2 Obiekt mapowy powinien być hierarchiczny z możliwością "drill-down".

19.1.2 Interfejs

19.1.2.1 Interfejs edytora map powinien umożliwiać wykonywanie następujących czynności:

19.1.2.1.1 Dodawanie/konfigurowanie obiektów mapy (takich jak kształty, obrazy i tekst).

19.1.2.1.2 Dodawanie zasobów obiektu do mapy (takich jak kamery, urządzenia integracyjne, zdarzenia).

19.1.2.1.3 Dodawanie akcji do obiektów mapy.

19.1.2.1.4 Łączenie się z obiektem (obiektami) i przeglądanie zasobów obiektu.

19.1.3 Funkcje

19.1.3.1 System powinien zawierać, lecz nie jest ograniczony do następujących funkcji kreatora map:

19.1.3.1.1 Kreator ustawień mapy oferujący funkcję szybkiego tworzenia.

19.1.3.1.2 Import grafiki w formacie JPG lub PNG.

19.1.3.1.3 Tworzenie hiperłączy z wnętrza mapy do innych map witryny.

19.1.3.1.4 Obiekty mapy mogą być skonfigurowane do wykonywania akcji na mapie po otrzymaniu określonych wyzwalaczy.

19.1.3.1.5 Warstwy mapy; Warstwy posiadają opcje przezroczystości / ukrycia - pokazania.

19.1.3.1.6 Możliwość powiązania warstw z predefiniowanymi pozycjami PTZ.

19.1.3.1.7 Możliwość włączania i wyłączania warstw w odpowiedzi na zdarzenie systemowe (np. wskazanie otwarcia/zamknięcia drzwi).

19.1.3.1.8 PTZ z powiązanymi, edytowalnymi Presetami.

19.1.3.1.9 Przeciąganie wszystkich dostępnych zasobów obiektu z listy zasobów obiektu bezpośrednio na mapę.

19.1.3.1.10 Dodawanie kamer metodą przeciągnij-i-upuść z ikonami (stałopozycyjne lub PTZ).

19.1.3.1.11 Dodawanie wejść/wyjść za pomocą ikony przeciągnij i upuść.

19.1.4 Akcje obiektów mapowych

19.1.4.1 Obiekty mapowe mogą być skonfigurowane tak, aby wykonywały określone akcje po otrzymaniu określonych wyzwalaczy. Przykłady wyzwalaczy, które mogą uruchomić akcję obiektu mapy obejmują, ale nie są ograniczone do następujących:

19.1.4.1.1 Kliknięcie lewym przyciskiem myszy w zakładce Mapa w interfejsie użytkownika VMS.

19.1.4.1.2 Kliknięcie prawym przyciskiem myszy w zakładce Mapa w interfejsie użytkownika VMS.

19.1.4.1.3 Zmiana danych wejściowych,

19.1.4.1.4 Zmiana stanu urządzenia,

19.1.4.1.5 Zdarzenia urządzenia integracyjnego.

19.1.4.1.6 Przykłady działań, które obiekty mapy mogą wykonać po otrzymaniu wyzwalacza obejmują, ale nie są ograniczone do następujących:

19.1.4.1.7 Podłączenie do Witryny,

19.1.4.1.8 Przejście do Presetu kamery,
19.1.4.1.9 Wykonać animację,
19.1.4.1.10 Wyświetlanie menu podręcznego,
19.1.4.1.11 Ustawianie wyjścia przekaźnikowego.

Mapy w interfejsie operatora VMS

19.1.5 System powinien umożliwiać wgranie map utworzonych w oprogramowaniu Map Editor i zapisanych do zakładki Mapy w interfejsie operatora VMS.

19.1.6 System powinien umożliwiać dodawanie wielu map do jednej lokalizacji.

19.1.7 System powinien opcjonalnie umożliwiać zdalnym użytkownikom automatyczny podgląd mapy obiektu.

19.1.8 System powinien umożliwiać zdalnym klientom pobieranie i przechowywanie map lokalnie, aby wyeliminować konieczność pobierania mapy dla każdego połączenia.

19.1.9 System powinien umożliwiać zarządzanie mapami witryn, co obejmuje:
19.1.9.1 Ustawienie domyślnej mapy,
19.1.9.2 Usuwanie map,
19.1.9.3 Dodawanie map.

19.1.10 System powinien umożliwiać, aby wszystkie akcje obiektów mapowych, które zostały skonfigurowane dla obiektu w oprogramowaniu Edytor Map były widoczne/działające/interaktywne (tam gdzie ma to zastosowanie) na mapie w interfejsie użytkownika VMS.

19.1.11 System powinien pozwalać użytkownikowi na:
19.1.11.1 Powiększanie/zmniejszanie mapy,
19.1.11.2 Przeciąganie i upuszczanie kamer z mapy na monitory w celu podglądu,
19.1.11.3 Ukrywanie/pokazywanie obiektów mapy,
19.1.11.4 Ukrywanie/pokazywanie/zmienianie przezroczystości warstw.

20 Aplikacja mobilna

Możliwości ogólne

20.1.1 System powinien udostępniać bezpłatną aplikację mobilną.

20.1.2 System nie powinien wymagać instalacji dodatkowego oprogramowania po stronie serwera, dodatkowych wtyczek lub specjalnego serwera mobilnego, aby umożliwić mobilne przeglądanie i przeglądanie materiałów wideo.

20.1.3 System powinien udostępniać tę aplikację w Apple iStore oraz Google Play Store.

20.1.3.1 Dostęp do niej powinien być możliwy poprzez interfejs HTTP.

20.1.4 Aplikacja powinna obsługiwać następujące funkcje:

20.1.4.1 Sterowanie kamerami za pomocą PTZ.

20.1.4.2 Przybliżanie/oddalanie.

20.1.4.3 Sterowanie wejściami/wyjściami.

20.1.4.4 Podgląd z wielu kamer (do czterech kamer).

20.1.4.5 Zapisywanie szczegółów dla wielu serwerów.

21 Interfejs programowania aplikacji

Możliwości ogólne

21.1.1 System powinien zawierać interfejs protokołu aplikacji (API), który powinien umożliwiać oprogramowaniu stron trzecich pobieranie informacji z systemu VMS i zarządzanie nimi, a także sterowanie zasobami systemu.

Informacje o wykazie miejsc

21.1.2 System powinien zawierać następujące elementy dotyczące informacji z wykazu obiektów:

21.1.2.1 Dostęp do witryny powinien być realizowany poprzez uwierzytelnienie typu digest i ograniczony w oparciu o wstępnie skonfigurowane poziomy dostępu użytkownika. API będzie mieć dostęp do szczegółów witryny poprzez serwer logowania. Obejmuje to nazwę witryny i jej unikalny numer identyfikacyjny.

21.1.3 System powinien zawierać następujące informacje dotyczące zasobów kamer:

21.1.3.1 API powinno zapewniać możliwość wylistowania wszystkich kamer i zasobów kamer na witrynie, z wyjątkiem:

21.1.3.1.1 Podania z formatami wideo, które nie są obsługiwane przez RTSP będą wyłączone z listy kamer API.

21.1.4 System powinien zawierać następujące informacje dotyczące informacji o zasilaniu kamer:

21.1.4.1 Nazwa,

21.1.4.2 Unikalny identyfikator,

21.1.4.3 Kanał audio (tak/nie),

21.1.4.4 Informacje o poziomie dostępu,

21.1.4.5 Status kamery "Online/Offline",

21.1.4.6 Status PTZ,

21.1.4.7 Informacje o wzorcach/ustawieniach wstępnych,

21.1.4.8 Informacje o ścieżce wideo na żywo,

21.1.4.9 Informacje o ścieżce przeglądania wideo.

21.1.4.10 Możliwość ponownego mapowania adresu IP serwera wewnętrznego, który API publikuje dla kamery.

21.1.4.11 Interfejs osi czasu.

21.1.5 System powinien zawierać następujące elementy w odniesieniu do strumieniowej transmisji obrazu na żywo:

21.1.5.1 API powinno umożliwiać strumieniowe przesyłanie obrazu z kamery na żywo, przy użyciu protokołu RTSP.

21.1.5.2 Strumieniowa transmisja wideo na żywo powinna wymagać uwierzytelnienia klienta.

21.1.5.3 Przełączanie kamer na monitory.

21.1.5.4 Strumieniowa transmisja webowa zgodna z HTTP/HTML5.

21.1.6 System powinien zawierać następujące elementy dotyczące przeglądu kamer:

21.1.6.1 API powinno pozwalać na przeglądanie zarejestrowanego materiału wideo.

21.1.6.2 Dostęp do nich powinien być realizowany poprzez protokół RTSP.

21.1.6.3 Interfejs API musi umożliwiać pobieranie przeglądanego materialu filmowego od określonej daty i godziny.

21.1.6.3.1 Jeżeli w podanym czasie nie ma materialu wideo, serwer zwróci material wideo najbardziej zbliżony do żądanego czasu.

21.1.6.4 API musi pozwalać na umieszczenie w żądaniu pola, które spowoduje, że sesja będzie transmitowana tak szybko, jak pozwoli na to klient/połączenie.

21.1.6.5 Obslugiwane będą następujące transporty strumieniowe:

21.1.6.5.1 RTP over UDP.

21.1.6.5.2 RTP po TCP.

21.1.7 System powinien zawierać następujące elementy dotyczące Audio Wywolania/ Sluchania:

21.1.7.1 API powinno pozwalać na strumieniowe przesyłanie niezależnych wejść i wyjść audio do i z wejść i wyjść audio na serwerze.

21.1.7.2 "Niezależny" oznacza tutaj, że dźwięk nie powinien być związany z obrazem.

21.1.7.3 Powinno to być dokonywane poprzez protokół SIP.

21.1.8 Interfejs API powinien umożliwiać następujące sterowanie kamerami PTZ:

21.1.8.1 Przesuwanie

21.1.8.2 Przejście do ustawienia wstępnego

21.1.8.3 Zapisywanie ustawienia wstępnego

21.1.8.4 Sterowanie ostrością/przysłona

21.1.8.5 Uruchomienie zaprogramowanego wzoru (trasa)

21.1.8.6 Sterowanie PTZ powinno odbywać się poprzez HTTP.

21.1.9 System powinien zapewniać następujące funkcje w zakresie zarządzania zasobami wejścia/wyjścia (HTTP; monitorowanie zmian stanu zasobów wejścia/wyjścia, sterowanie wyjściami):

21.1.9.1 API powinno wspierać monitorowanie wszystkich wejść/wyjść w obiekcie.

21.1.9.2 Na żądanie API udostępni wszystkie bieżące We/Wy witryny.

21.1.9.3 API będzie również utrzymywać otwarte połączenie, tak dlugo jak klient sobie tego zażyczy, i aktualizować zasoby We/Wy poprzez to połączenie. Aktualizacje te będą:

21.1.9.3.1 Zmiany stanu zasobów.

21.1.9.3.2 Dodanie zasobu

21.1.9.3.3 Usunięcie zasobu

21.1.9.3.4 Modyfikacja zasobu (zmiana nazwy)

21.1.9.3.5 Elementy sterujące wyjściami powinny być ustawione, wyczyszczone i impulsowe.

21.1.10 System powinien uwzględniać następujące elementy dotyczące odbierania zdarzeń/alarmów technicznych:

21.1.10.1 Interfejs API powinien umożliwiać odbieranie alarmów z serwera. Zarówno Alarmy Techniczne (alarmy związane z funkcjonowaniem obiektu), jak i Alarmy Zdarzeniowe (alarmy wyzwalane przez zdarzenia VMS i We/Wy).

21.1.10.2 Serwer powinien dostarczać następujące informacje o alarmach:

21.1.10.2.1 Identyfikator obiektu źródłowego.

21.1.10.2.2 Nazwa lokalizacji źródlowej.

21.1.10.2.3 Typ alarmu (techniczny/zdarzenie).

21.1.10.2.4 Nazwa alarmu.

21.1.10.2.5Skojarzone zasoby kamery.