WYMAGANIA OGÓLNO-FUNKCJONALNE OPROGRAMOWANIA DO ZARZĄDZANIA SYSTEMEM WIDEO (VMS)

Spis treści

1. WYMAGANIA OGÓLNE

Rozwiązanie musi być kompatybilne z ogólną infrastrukturą klient-serwer, zasobami i systemami oraz skalowalne i elastyczne w dostosowywaniu się do zmian i potrzeb operacyjnych. Rozwiązanie musi obsługiwać funkcje audytu i identyfikowalności dla interakcji z użytkownikiem i przepływów pracy inicjowanych przez system. Rozwiązanie musi być wyposażone w środki odporności na awarie systemu i punktów, aby zmaksymalizować ciągłość działania i zminimalizować zakłócenia operacyjne.

VMS musi działać w architekturze federacyjnej umożliwiającej każdemu upoważnionemu użytkownikowi bezproblemowy dostęp do zasobów systemowych (takich jak wideo na żywo/nagrane) podłączonych do dowolnego serwera sieciowego. Architektura federacyjna umożliwi również scentralizowaną administrację serwerów aplikacji, aplikacji klienckich i koderów/aparatów cyfrowych w celu aktualizacji oprogramowania, oprogramowania układowego, dystrybucji alarmów i alertów oraz tworzenia kopii zapasowych danych konfiguracyjnych.

VMS będzie działał na standardowych systemach operacyjnych Windows i różnych mobilnych systemach operacyjnych dla platform opartych na aplikacjach mobilnych.

Licencjonowanie (lub rozbudowa i modyfikacja zasięgu systemu CCTV) nie może być nadmiernie skomplikowane. Proces nie powinien wymagać wielu licencji na wdrożenie dodatkowych urządzeń peryferyjnych. Rozwiązanie musi być zgodne ze standardami IP, branży, prawnymi i regulacyjnymi w zakresie projektowania, budowy i eksploatacji.

Rozwiązanie musi być w stanie:

- zapewnić transmisję strumieniową na żywo materiału wideo,
- nagrywanie, przechowywanie i zarządzanie danymi wideo,
- sterowanie urządzeniami peryferyjnymi i zasobami podłączonymi do VMS,
- zapewnić środki komunikacji między użytkownikami a systemem,
- spełniać wymagania w zakresie cyberbezpieczeństwa w zakresie jego budowy i integracji sieci,
- zapobiegać nieuprawnionemu użyciu,
- zapewnienie identyfikowalności działań użytkownika.

Rozwiązanie musi posiadać ramy usług konserwacji i naprawy wsparcia, aby zapewnić integralność systemu, bezpieczeństwo i ciągłość działania.

Rozwiązanie musi być zaprojektowane i działać w środowisku zoptymalizowanym pod kątem architektury federacyjnej dostosowanej do typów i liczby śladów wideo w różnych lokalizacjach, które dział musi obsługiwać.

Rozwiązanie musi być wspierane przez szkolenia użytkowników i powiązane cyfrowe narzędzia szkoleniowe.

Rozwiązanie musi posiadać funkcjonalność promującą łatwość obsługi, działać na zasadzie minimalnych interakcji użytkownika w obsłudze systemu oraz być intuicyjne w obsłudze.

2. EFEKTYWNOŚĆ I ZARZĄDZANIE ZASOBAMI

VMS musi być zdolny do działania na standardowym, gotowym sprzęcie sieci LAN/IP, serwerze i pamięci masowej. VMS nie może wymagać żadnej konkretnej marki/modelu zastrzeżonego sprzętu.

VMS musi akceptować strumienie wideo IP z koderów i zasobów kamer dowolnej marki.

VMS musi być zintegrowany z istniejącą infrastrukturą serwerów fizycznych oraz z istniejącymi cyfrowymi urządzeniami rejestrującymi i infrastrukturą pamięci masowej użytkownika.

VMS musi akceptować zarówno strumienie o zmiennej, jak i stałej szybkości transmisji bitów z podłączonych kamer/koderów.

Urządzenia sterujące aplikacją VMS nie mogą wymagać specjalnego programowania technicznego na samym urządzeniu. Te wymagania programistyczne muszą mieścić się w możliwościach aplikacji VMS.

Urządzenia sterujące VMS nie mogą być ograniczone do określonych marek i muszą być kompatybilne z innymi zasobami użytkownika.

Aplikacja kliencka VMS musi obsługiwać co najmniej 10 monitorów płasko ekranowych podłączonych do jednego komputera.

VMS będzie obsługiwał szereg niezależnych typów kompresji strumienia.

VMS będzie kompatybilny ze standardami SMPTE HD 296M, 274M i UHDTV standard 2036-1.

Wszystkie aplikacje VMS powinny działać na serwerach.

VMS będzie obsługiwany przez Software Development Kit (SDK) lub podobny, który jest regularnie aktualizowany, w pełni funkcjonalny i zapewnia dostęp do programowania stron trzecich do celów integracji VMS.

VMS musi być kompatybilny z istniejącymi enkoderami różnych producentów.

Funkcje kodera i kamery muszą być dostępne za pośrednictwem interfejsu użytkownika VMS.

VMS musi być kompatybilny z szeregiem cyfrowych kamer, a także z rozwiązaniami SD i HD.

Wszystkie kamery podłączone do VMS muszą być sterowane przez dowolne urządzenie wejściowe. Obejmuje to między innymi mysz, joysticki, panele sterowania, ekran dotykowy, urządzenia mobilne lub urządzenia wejściowe z klawiaturą.

VMS musi mieć konfigurowalną automatyczną regulację szybkości transmisji bitów w celu dostosowania do dostępności przepustowości.

VMS musi automatycznie kompresować dane w sytuacjach mniejszej przepustowości, aby zapewnić optymalny poziom jakości dla liczby przeglądanych urządzeń peryferyjnych.

VMS musi działać na serwerach wirtualnych, aby zoptymalizować możliwości przetwarzania, skalowalność i elastyczność w zarządzaniu awariami sieci lub komponentów serwera.

VMS będzie miał konfigurowalne ustawienia dla zmiennych zasad przechowywania nagrań, wielowarstwowych funkcji zasad i kategoryzacji nagrań.

VMS będzie miał możliwość "przerzedzania" danych, aby sprostać ograniczeniom przepustowości transmisji strumieniowej na żywo i wydłużyć czas przechowywania danych poprzez niestandardowe, stopniowe, częściowe usuwanie klatek wideo.

VMS będzie miał możliwość ustawienia przypisania aktywów, które można skonfigurować do dowolnej kombinacji znaków zmiennych zgodnie z wymaganiami użytkownika.

VMS będzie miał konfigurowalne ustawienia dla zmiennych zasad przechowywania nagrań i kategoryzacji nagrań.

3. ZDOLNOŚĆ AUDYTÓW

VMS musi być zsynchronizowany z istniejącym źródłem NTP (Network Time Protocol) dostosowanym do innych systemów użytkownika.

VMS musi posiadać dziennik inspekcji przepływów pracy i interakcji użytkowników i systemu.

VMS musi dokumentować wszystkie zmiany związane z użytkownikiem w aplikacji i podłączonych urządzeniach peryferyjnych ze środowiskiem aplikacji.

VMS musi rejestrować, wraz z identyfikatorem, interakcje użytkowników, które mają wyższe uprawnienia z nimi skojarzone.

VMS będzie w stanie rejestrować i różnicować dane wejściowe użytkowników w sytuacjach, gdy wielu użytkowników przegląda i kontroluje tę samą grupę urządzeń w tym samym czasie.

VMS będzie obsługiwał rejestrowanie interakcji na interfejsie graficznym przez użytkownika, wyzwalanych przez reguły biznesowe lub poprzez aktywację użytkownika.

4. CIĄGŁOŚĆ i NIEZAWODNOŚĆ PRACY

Rozwiązania przełączania awaryjnego VMS muszą zapewniać użytkownikom płynne przełączanie bez istotnych zakłóceń.

VMS musi być zdolny do rozbudowy lub modyfikacji lokalnie lub globalnie bez zakłóceń w normalnej wydajności operacyjnej.

VMS będzie bezproblemowo przesyłać lokalnie przechowywane dane wideo z powrotem do głównej infrastruktury pamięci masowej systemu, aby uniknąć wpływu na operacje.

VMS musi inicjować i koordynować przepływy pracy trybu failover, w tym:

- serwery aplikacji VMS,

- pamięć masowa (na poziomie VMS),

- zasilanie (na poziomie VMS).

VMS musi posiadać następujące funkcje przełączania awaryjnego nieodłącznie związane z systemem:

- zakłócenie warstwy aplikacji VMS,

- zakłócenia w pracy serwerów aplikacji VMS.

VMS musi zapewniać automatyczne alerty i powiadomienia o awariach i awariach systemu, od poszczególnych urządzeń peryferyjnych po infrastrukturę serwerową.

VMS musi mieć możliwość wysyłania alertów i powiadomień zewnętrznie do użytkowników niezalogowanych do VMS.

VMS musi inicjować tworzenie kopii zapasowych systemu i danych zgodnie z konfiguracją użytkownika.

Wyzwalacze tworzenia kopi mogą obejmować:

- system,

- przed jakimikolwiek aktualizacjami, uaktualnieniami lub modyfikacjami wystąpień aplikacji,

- przed jakimkolwiek zamknięciem systemu,

- dane wideo,

- materiał filmowy i dane z zakładek,

- wyodrębnione materiały filmowe i dane,

- ręcznie oznaczone materiały filmowe i dane,

- generowany system (poprzez alerty, alarmy, analizy).

VMS podejmie próbę samodzielnego segregowania i rozwiązywania problemów systemowych, peryferyjnych i awarii połączeń. Metody samoadresowania powinny obejmować:

- ponowne uruchamianie komponentów,

- ponawianie prób połączeń,

- odświeżanie danych.

Awarie połączeń i akcje autosegregujące będą rejestrowane do celów rozwiązywania problemów i inspekcji.

VMS automatycznie skopiuje nagrane wideo do lokalizacji przechowywania w trybie gotowości, w tym obsługiwanych urządzeń peryferyjnych (wideoenkoderów i aparatów cyfrowych), i przywróci materiał wideo z powrotem na główny nośnik danych serwera po naprawie systemu nagrywania lub awarii sieci.

Dane w trybie gotowości powinny być przywracane w sposób bezproblemowy, aby nie zakłócać pracy użytkownika.

VMS ułatwi nagrywanie wysokiej jakości nawet wtedy, gdy strumienie na żywo mogą być zagrożone przez problemy z przepustowością, siecią lub aplikacją.

5. ZGODNOŚĆ

Producent VMS musi być aktualnym członkiem Open Network Video Interface Forum (ONVIF), a oferowany VMS musi być w pełni kompatybilny z urządzeniami wideo IP z certyfikatem ONVIF.

6. ZDOLNOŚĆ OPERACYJNA

VMS musi być w stanie obsłużyć więcej niż 15 000 wejść wideo, 500 stacji roboczych do przeglądania w różnych lokalizacjach w ponad 200 geograficznie niezależnych lokalizacjach oraz nieograniczony dostęp do przeglądania mobilnego (w Internecie lub w inny sposób). VMS musi być w stanie nagrywać z prędkością co najmniej 12 obrazów na sekundę.

Graficzny interfejs użytkownika VMS (GUID) musi mieć wspólny zbiór zdarzeń alarmowych, który autoryzowani użytkownicy mogą wykonać lub przydzielić innemu użytkownikowi. Zdarzenie alarmowe, jeśli jest skojarzone z kamerą, musi automatycznie wyświetlać wideo ze scen przed i po alarmie (w trybie pauzy) wraz z obrazem na żywo z tej samej kamery. Musi istnieć możliwość ręcznego potwierdzenia przez użytkownika lub zainicjowania potwierdzenia systemu po określonym czasie.

VMS musi obsługiwać funkcję wielokrotnego castingu, a także możliwość emisji pojedynczej dla każdego urządzenia peryferyjnego kamery w wielu instancjach jednocześnie.

VMS musi być w stanie wyświetlać na monitorach ściennych, które są w pełni niezależne od jakiejkolwiek stacji roboczej i mogą być kontrolowane przez wielu upoważnionych użytkowników jednocześnie.

Funkcja wykrywania ruchu VMS rozróżni ruch i kierunek ruchu między ludźmi i obiektami.

VMS będzie mógł zintegrować się z innymi systemami i zainicjować przepływy pracy w celu wysyłania wiadomości w formie wiadomości e-mail, SMS lub podobnych środków.

VMS musi zapewniać możliwość wyświetlania danych wideo z urządzeń peryferyjnych i sterowania takimi urządzeniami (z zastrzeżeniem uprawnień użytkownika) ze wszystkich systemowych punktów dostępu do wyświetlania na wszystkich obsługiwanych platformach VMS.

VMS musi umożliwiać strumieniowe przesyłanie materiału wideo do dowolnego autoryzowanego punktu dostępu za pośrednictwem sieci CCTV.

VMS musi być w stanie nagrywać materiał wideo na żywo za pośrednictwem dowolnego urządzenia peryferyjnego do nagrywania w sieci CCTV.

VMS musi być w stanie odtwarzać nagrany materiał filmowy, który jest przechowywany w sieci CCTV.

VMS musi mieć możliwość konfigurowania urządzeń peryferyjnych niezależnie od innych urządzeń peryferyjnych (z zastrzeżeniem reguł użytkownika), zgodnie z lokalizacjami, regionami lub na poziomie globalnym i musi obejmować, ale nie może być ograniczony do takich parametrów jak:

- liczba klatek na sekundę,

- przepustowość,

- jakość obrazu,

- interwał klatek kluczowych,

- rozdzielczość,

- profile użytkowników,

- ustawienia grupy użytkowników,

- wstępnie ustawione pozycje dla widoków kamery,

- preferencje tworzenia kopii zapasowych,

- preferencje alarmów i alertów,

- zakładki,

- wyodrębnianie raportów,

- ekstrakcja danych wideo,

- preferencje samodzielnego segregowania i prostowania,

- blokada i hierarchia użytkowników,

- zmienna szybkość transmisji i ustawienia jakości wideo.

VMS musi posiadać środki do zarządzania dostępem użytkowników do urządzeń peryferyjnych i kontroli nad nimi zgodnie z hierarchią dostępu kontrolnego ustanowioną i skonfigurowaną przez użytkownika.

VMS musi współpracować i przetwarzać zdarzenia alarmowe, których użytkownik wymaga w źródłach programowania (wysokiego poziomu), analizy wideo i urządzeń (niskiego poziomu).

VMS musi mieć możliwość konfigurowania wstępnie ustawionych scen (wstępnie skonfigurowanych i skoordynowanych widoków kamery oraz automatycznej konfiguracji innych powiązanych ustawień VMS, takich jak automatyczne kopie zapasowe), które wyzwalają różne alerty i alarmy lub które można zainicjować ręcznie.

Po aktywacji wstępnie ustawionych scen VMS musi być w stanie aktywować kamery, aby ustawić ostrość na obiektach lub osobach, zainicjować nagrywanie lub zainicjować przepływ pracy systemu, jeśli ruch zostanie wykryty na wybranych strumieniach kamer. Sceny muszą również dotyczyć widoków kamery, koordynacji urządzeń peryferyjnych, kopii zapasowych, zakładek i śledzić przepływy pracy z systemu.

VMS musi być w stanie dodać do zakładek dane CCTV i materiał wideo przed alarmem i po alarmie, z możliwością konfiguracji typów alarmów i alertów, które wyzwalają nagrywanie. Nagrania wyzwalane przez alerty i alarmy muszą być zapisywane w miejscu, które ma wyższy priorytet niż standardowe przechowywanie danych CCTV.

VMS zapisze się w osobnej pamięci masowej, materiał filmowy, który jest dodawany do zakładek w miejscach, które mają wyższy priorytet niż standardowe przechowywanie danych CCTV.

VMS będzie miał funkcje ustawienia ręcznego potwierdzania przez użytkownika lub automatycznego potwierdzania po zdefiniowanym okresie.

VMS musi wspierać w ustalaniu reguł na poziomie aplikacji, w celu określenia, w jaki sposób zarejestrowane dane są traktowane priorytetowo, przechowywane, jaki jest czas przechowywania i środki bezpieczeństwa wokół takich przechowywanych danych.

VMS musi zapewniać funkcje optymalizacji i zarządzania połączeniami zdalnymi za pośrednictwem łączy o niskiej przepustowości.

VMS musi umożliwiać użytkownikom przeglądanie i kontrolowanie urządzeń peryferyjnych za pośrednictwem platformy, która może działać w szerokim zakresie systemów i która nie jest oparta na aplikacjach komputerowych.

VMS musi mieć możliwość tworzenia zakładek materiału filmowego na żywo lub podczas odtwarzania, z konfigurowalnymi skrótami klawiszowymi, skrótami, aktywacją w interfejsie użytkownika lub inicjowanym przez system.

Zakładki generowane przez użytkownika i system muszą być dostępne dla grup użytkowników skonfigurowanych przez system i muszą być używane do korelowania zdarzeń lub zapisywania znaczników czasu do wykorzystania w przyszłości.

Funkcja zakładek VMS musi mieć możliwość różnicowania kategorii zakładek, którą można konfigurować w celu dostosowania do zmieniających się potrzeb użytkownika.

VMS musi posiadać hierarchię systemową priorytetów użytkownika, zapewniającą użytkownikom wyższy priorytet kontroli nad urządzeniami peryferyjnymi i możliwość zablokowania dostępu do kamer, aby uniknąć konfliktów kontroli urządzeń peryferyjnych.

VMS musi mieć funkcję zastępowania dla swojej funkcji blokowania sterowania.

VMS musi umożliwiać upoważnionym pracownikom działu jednoczesne oglądanie na żywo i odtwarzanie obrazów w konfiguracji wieloekranowej na tym samym komputerze klienckim, zarządzanie eksportem i ustawieniami wstępnymi/sekwencjami, a także eksportowanie w dowolnym dostępnym formacie danych eksportowych.

VMS musi mieć standardowo lub za pośrednictwem interfejsów programowania aplikacji (API) do różnych programów, funkcję wykrywania ruchu osób i obiektów.

VMS musi mieć konfigurowalne zsynchronizowane lub niezsynchronizowane nagrywanie i możliwość przesyłania strumieniowego na żywo.

VMS będzie obsługiwał konfigurowalne skrypty lub makra, które mogą być uruchamiane automatycznie w odpowiedzi na różne zdarzenia alarmowe. VMS będzie można zaprogramować tak, aby umożliwić automatyczne przeprowadzanie z góry określonej sekwencji zdarzeń w odpowiedzi na alarmy. Obejmuje to automatyczny wybór wielu kamer do wstępnie zaprogramowanego monitora i automatyczne pozycjonowanie kamer PTZ za pomocą wstępnie ustawionego przywołania.

Alarmy będą mogły być przesyłane do przepływu pracy do dowolnego punktu kontaktu w sieci CCTV i poza siecią CCTV w celu uzyskania akcji lub informacji.

VMS będzie w stanie pobierać nagrane wideo na podstawie kryteriów wyszukiwania użytkowników, w tym kombinacji:

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

VMS zbuduje pojedynczy, złożony plik do eksportu zawierający sekwencję wybranych nagrań z kamer, w których materiał musi być zbudowany z wielu sekwencji, kamer i pól widzenia w czasie.

VMS będzie mógł odbierać żądania użytkowników dotyczące eksportu danych wideo i mieć zautomatyzowane przepływy pracy dla eksportu, w których istnieją reguły biznesowe.

VMS będzie miał własne wrodzone możliwości lub wspierające interfejsy API do integracji z elektronicznymi systemami kontroli dostępu.

VMS będzie miał własne nieodłączne możliwości lub obsługujące interfejsy API do integracji z obiektami i analizą wideo OCR (Optical Character Recognition).

VMS będzie miał własne możliwości lub wspierające interfejsy API do integracji z analizą wideo rozpoznawania twarzy.

VMS będzie miał własną zdolność lub za pośrednictwem interfejsów API do integracji z funkcją automatycznego śledzenia osób lub obiektów, zmapowanych do sieci CCTV w całej lokalizacji i konfigurowalnych przez Zamawiającego.

VMS będzie miał własne możliwości lub za pośrednictwem interfejsów API do integracji z automatyczną analizą wideo rozpoznawania tablic rejestracyjnych pojazdów (ANPR) (przy użyciu OCR).

VMS będzie miał automatycznie generowane przez system przepływy pracy, które inicjują się na wykrytych przez system zdarzeniach. Może to obejmować, w razie wykrycia zdarzeń, przedmiotów lub osób:

- dodawanie zakładek do nagrań, powiązanych informacji o systemie, dzienników audytu, dzienników systemowych i metadanych,
- przechwytywanie zdjęć,
- alerty i powiadomienia,
- bezpieczna kopia zapasowa danych.

VMS będzie w pełni dostępny na mobilnych systemach operacyjnych Android i Apple.

Tam, gdzie pozwalają na to zasady i przepisy, VMS będzie miał możliwość integracji 1- lub 2-stronnej komunikacji głosowej w celu obsługi funkcji wideo w różnych lokalizacjach w zależności od potrzeb użytkownika.

VMS będzie w stanie rejestrować obrazy oraz automatycznie optymalizować i udoskonalać jakość obrazu w konfigurowalnej liczbie zdjęć, automatycznie dostosowując się do punktu ogniskowego, oświetlenia i ustawień otoczenia.

VMS będzie w stanie odróżnić ruch między osobami, elementami naturalnymi lub przedmiotami.

VMS będzie integrować się z mobilnymi urządzeniami peryferyjnymi kamer, działającymi w mobilnej sieci użytkownika, takimi jak:

- ręczne kamery,
- kamery i urządzenia audio,
- kamery nasobne na korpusie/nakryciach głowy.

VMS pomieści dane wideo z mobilnych urządzeń peryferyjnych, takich jak telefon komórkowy i zintegruje takie dane z szerszym systemem nadzoru wideo.

VMS będzie mógł eksportować materiał wideo w różnych formatach za pośrednictwem portalu internetowego, na którym może działać, dla wewnętrznych i zewnętrznych upoważnionych użytkowników.

7. BEZPIECZEŃSTWO SYSTEMU

VMS musi działać z indywidualnymi kontami użytkowników. Poświadczenia haseł do kont użytkowników muszą być zmieniane minimum co 6 miesięcy.

Dostęp do VMS musi być uzyskiwany przez użytkowników za pośrednictwem uwierzytelniania wieloskładnikowego, dlatego aplikacja musi mieć własny proces uwierzytelniania oprócz innych procesów logowania do działu, aby uzyskać dostęp do urządzenia.

Wszystkie interakcje użytkowników z aplikacjami VMS muszą opierać się na uprawnieniach grup użytkowników (np. administratorzy globalni/witryny, użytkownicy ogólni, użytkownicy wyższej kategorii, użytkownicy tylko do odczytu itp.). Te uprawnienia i grupy muszą być konfigurowalne zgodnie z wymaganiami użytkownika.

VMS może zezwalać tylko grupom użytkowników z przypisanymi odpowiednimi uprawnieniami na wyodrębnianie danych z systemu.

VMS musi obsługiwać co najmniej 128-bitowe szyfrowanie danych (lub silniejsze) między urządzeniami brzegowymi (kamerami lub enkoderami) a urządzeniami nagrywającymi/wyświetlającym.

Dane VMS będą można wyodrębnić poza system tylko na zewnętrznych urządzeniach pamięci masowej zatwierdzonych przez użytkownika. Nieautoryzowani użytkownicy, którzy uzyskają dostęp do urządzenia, nie będą mogli przeglądać, modyfikować ani wykorzystywać przechowywanych w nich danych.

Aplikacja VMS, na dowolnej platformie, będzie miała funkcję, która zasłania informacje na ekranie, konfigurowalną do czasu bezczynności.

8. WSPARCIE I SERWIS

VMS będzie miał możliwość samodzielnego monitorowania stanu aplikacji, powiązanych urządzeń peryferyjnych kamer i enkoderów, infrastruktury serwerów i pamięci masowej.

Oprogramowanie klienckie VMS będzie utrzymywać dedykowane pliki dziennika systemowego w dowolnej wyznaczonej lokalizacji plików sieciowych i rejestrować chronologię działań i zdarzeń systemu aplikacji, odpowiednią do użycia w rozwiązywaniu błędów aplikacji klienckiej.

Dane z inicjowania zgłoszeń muszą być również rejestrowane i analizowane przez system, aby zapewnić wgląd w ciągłe doskonalenie i ulepszone odpowiedzi wsparcia.

VMS będzie zbierać dane o incydentach i plikach dziennika oraz raportować spostrzeżenia, które pomogą w ciągłym doskonaleniu.

Gdy problemy systemowe mają wpływ na VMS, VMS zainicjuje i wyda zgłoszenia na podstawie wagi i czasu trwania problemu, w oparciu o wymagania użytkownika. Zostanie to zgłoszone do użytkownika w sposób zautomatyzowany.

9. SZKOLENIE UŻYTKOWNIKÓW

VMS musi być wspierany przez kompleksowe i zaplanowane ramy szkoleń, które są dostosowane do potrzeb użytkownika. Zdolność do oceny szkoleń musi być dostępna w celu wsparcia wprowadzania i bieżącej obsługi użytkowników systemu.

Szkolenia muszą być prowadzone osobiście dla różnych grup użytkowników, wyznaczonych z regionów, witryn i grup użytkowników w różnych środowiskach, aby skutecznie dotrzeć do użytkowników końcowych.

VMS musi zawierać kompleksowe samouczki pomocy dla użytkowników dostępne za pośrednictwem aplikacji klienckiej. Te samouczki muszą być indeksowane i zawierać tematy pomocy, które można przeszukiwać za pomocą słów lub fraz kluczowych.

10. WRAŻENIA I ODCZUCIA UŻYTKOWNIKÓW

VMS musi być wyposażony w dobrze zaprojektowany i intuicyjny graficzny interfejs użytkownika (GUID), aby dostosować się do wymagań użytkownika.

VMS musi obsługiwać wyświetlanie wieloekranowe z konfigurowalnymi układami, a tam, gdzie przełączanie między widokami jest aktualnie wykonywane, występują one z minimalnym opóźnieniem lub przerwą podczas procesu przełączania.

VMS musi obsługiwać środki do łatwego konfigurowania ekranów, konfigurowania hierarchii widoków kamer, sekwencji tego, co jest wyświetlane na każdym ekranie, oraz konfigurowalnego układu okna, aby umożliwić użytkownikowi dostosowanie układu i zapisanie w swoim profilu.

Kolor, rozmiar i położenie metadanych identyfikacyjnych na materiale filmowym, który jest wyodrębniony lub odtwarzany, powinny być zmienne i konfigurowalne przez administratora.

Identyfikator GUID ma być konfigurowalny, aby przyciski, przełączniki aktywacji i elementy sterujące na identyfikatorze GUID mogły być przestawiane w różnych układach na ekranie.

VMS umożliwi logowanie użytkowników w sposób, który zoptymalizuje czas i włożony wysiłek związany z uwierzytelnianiem. VMS musi zezwalać wielu użytkownikom na logowanie się. Wylogowanie jednego użytkownika nie spowoduje zamknięcia ani wylogowania z aplikacji VMS, jeśli inni użytkownicy pozostaną zalogowani.

VMS będzie miał możliwość posiadania wielu widoków kamery na ekran/okno, a następnie możliwość używania skrótów klawiszowych do przełączania się między oknami na różnych ekranach, aby móc monitorować wiele obszarów i widoków w krótkim odstępie czasu.

VMS musi mieć możliwość tymczasowego odrzucenia alertu, gdy alert jest nadal aktywny i można go pobrać. Alert zostanie następnie ponownie wyświetlany po pewnym czasie.

VMS musi mieć zarówno wskaźniki wizualne, jak i alarmy dźwiękowe po zainicjowaniu.

Aplikacja VMS będzie miała konfigurowalne, wstępnie ustawione interfejsy wyświetlania i układy GUID, dostosowywane przez użytkownika, z predefiniowanymi ustawieniami specyficznymi dla danych logowania użytkownika. Ustawienia wstępne będą konfigurowalne, aby można je było zmieniać w zależności od czasu lub wykrycia zdarzenia.

Następujące informacje będą wyświetlane na wszystkich nagraniach i wyświetlaczach monitorów na żywo:

- czas systemowy (w formacie dwudziestoczterogodzinnym czasu lokalnego w stosunku do danej witryny),
- data systemowa (DD/MM/RRRR),
- identyfikator kamery,
- opis alfanumeryczny kamery,
- odniesienie do alertu/alarmu,
- odniesienie do sekwencji,
- odniesienie do sprawy.

VMS będzie miał konfigurowalne mapowanie witryny zasobów oraz wspomagające/predykcyjne mapowanie sekwencji kamer, aby ostrzec użytkowników o potencjalnym przełączaniu peryferyjnym kamery na podstawie zmapowanych tras przez witrynę.

Urządzenia peryferyjne będą widoczne w interfejsie graficznym użytkownika jako mapa specyficzna dla witryny i musi istnieć funkcjonalność „kliknij, aby wyświetlić”.