Especificación abreviada de A&E de CathexisVision 2020

Contenido

1 Introducción

Este documento es un resumen de los requisitos generales para el software de gestión de vídeo CathexisVision (que en adelante se denominará "el VMS") y/o los dispositivos periféricos producidos por Cathexis Technologies y suministrados por los distribuidores de Cathexis en determinadas regiones.[1] Para conocer las especificaciones completas, consulte las especificaciones íntegras de CathexisVision A&E.

Para cualquier consulta, póngase en contacto con support@cat.co.za.

[1] Aunque Cathexis ha hecho todo lo posible para asegurar la exactitud de este documento, no hay garantía de su exactitud, ni explícita, ni implícita. Las especificaciones están sujetas a cambios sin previo aviso.

2 Arquitectura del sistema

2.1 Arquitectura del sistema

2.1.1 El sistema de grabación y gestión de vídeo estará gestionado por el software de gestión de vídeo (VMS) y será de naturaleza cliente-servidor y constará de los siguientes componentes:

2.2 Servidores de grabación

2.2.1 Los servidores de grabación deberán gestionar lo siguiente:

2.2.1.1 Gestión de cámaras IP, dispositivos de E/S de red y codificadores de vídeo.

2.2.1.2 Grabación de vídeo en el almacenamiento y las bases de datos seleccionadas, ya sean locales o de red.

2.2.1.3 Gestionar la distribución de vídeo en vivo a servidores de clientes, clientes móviles y Video Walls.

2.2.1.4 Facilitar la búsqueda y revisión del vídeo grabado.

2.2.1.5 Gestionar los eventos técnicos o definidos por el usuario, las alarmas, sus disparadores y las acciones.

2.2.1.6 Análisis de vídeo en las cámaras seleccionadas.

2.2.1.7 Configuración y gestión de la integración de ANPR y de terceros.

2.2.1.8 Gestión de los derechos de acceso de los usuarios.

2.2.2 El sistema deberá permitir la asociación de múltiples servidores de grabación para formar un sitio. Estos servidores pueden estar ubicados geográficamente en uno o varios sitios físicos.

2.2.3 No será necesario un "servidor de gestión". Uno de los servidores de grabación se designa automáticamente como servidor de "gestión" o "maestro" para esta función.

2.2.4 No será necesario un servidor de análisis de vídeo. Esta función debe ser realizada por los servidores de grabación.

2.2.5 El software del servidor de grabación deberá ser compatible con los sistemas operativos Windows y Linux.

2.3 Servidores de cliente

2.3.1 El software del servidor de cliente deberá ser compatible con los sistemas operativos Windows y Linux.

2.3.2 El software del servidor de cliente deberá facilitar lo siguiente:

2.3.2.1 Realizar todas las funciones de instalación y configuración del sitio, que puede contener múltiples servidores de grabación.

2.3.2.2 Visualizar y revisar todas las cámaras del sitio.

2.3.2.3 Conectarse al portal de gestión de alarmas para ver y gestionar las alarmas de uno o varios emplazamientos.

2.3.2.4 Controlar las funciones del Video Wall a través de un panel Mímico.

2.3.2.5 Configuración y gestión de mapas de sitio.

2.3.2.6 Visualización y gestión de ANPR y otras bases de datos de integración.

2.3.2.7 Ver y gestionar las bases de metadatos.

2.4 Servidores de Video Wall

2.4.1 Los servidores de Video Wall deben acomodar el software de Video Wall para:

2.4.1.1 Acomodar múltiples servidores, cada uno de ellos capaz de acomodar múltiples monitores, cuya cantidad dependerá del hardware.

2.4.1.2 Mostrar hasta 64 vistas de cámara en cada monitor por instrucción del VMS.

2.4.1.3 Visualizar hasta 64 flujos de vídeo por monitor según las instrucciones del VMS.
2.4.1.4 Ejecutar recorridos de cámaras y recorridos de trazados (salvo).
2.4.1.5 Ser controlado a través de un Panel Mímico dentro del software de cliente del VMS.

2.5 Servidor de Failover

2.5.1 Los servidores de Failover adoptarán toda la funcionalidad de los servidores de grabación en caso de que un servidor de grabación falle o se desconecte.
2.5.2 Los servidores de Failover también facilitarán la Failover mediante la reinstalación automática de un servidor sustituido o reparado.
2.5.3 La Failover deberá ser de **naturaleza "hotspare".**
2.5.4 Podrán instalarse varios servidores de Failover en un mismo emplazamiento.
2.5.5 El tiempo de Failover debe ser configurable y no debe exceder los 30 segundos.

2.6 Portal de Gestión de Alarmas

2.6.1 El software del portal de gestión de alarmas deberá ser compatible con los sistemas operativos Windows y Linux.
2.6.2 El software del Portal de Gestión de Alarmas deberá recibir alarmas de múltiples sitios con múltiples servidores y tener procedimientos configurables para manejarlas.
2.6.3 El portal de alarmas deberá realizar el enrutamiento y la gestión de la conexión para la conexión automática y la transmisión de vídeo desde los sitios, cuyo detalle estará determinado por la alarma específica que se reciba.

2.7 Almacenamiento y bases de datos

2.7.1 El sistema deberá ser capaz de dividir las bases de datos en múltiples discos y/o dispositivos de almacenamiento en red.
2.7.2 Deberá ser compatible con los protocolos de almacenamiento más comunes, como SATA, SAS, SSD, DAS, SAN, NAS e iSCSI.
2.7.3 El sistema deberá proporcionar un sistema de base de datos propio para el almacenamiento de vídeo, y no depender de bases de datos de terceros (como MySQL) para esta función.
2.7.4 El sistema deberá ser capaz de crear bases de datos dedicadas, incluyendo:

2.7.4.1 Base de datos de vídeo general.
2.7.4.2 Base de datos de metadatos (integración).
2.7.4.3 Base de datos de eventos del sistema.
2.7.4.4 Base de datos de integración ANPR.
2.7.4.5 Base de datos de clasificación de objetos.

2.7.5 Todas las bases de datos deberán ser capaces de lo siguiente:

2.7.5.1 Reproducir vídeo desde un reproductor de vídeo integrado.
2.7.5.2 Filtrar y buscar entradas en las bases de datos.
2.7.5.3 Visualizar superposiciones y/o metadatos asociados a la grabación.
2.7.5.4 Exportación de las entradas de la base de datos en formato PDF o CSV.
2.7.5.5 Archivar el vídeo y los metadatos asociados desde el reproductor de vídeo integrado.
2.7.5.6 Envejecimiento del vídeo. Las secuencias de vídeo de una base de datos pueden transcodificarse a un tamaño reducido y almacenarse durante más tiempo en una segunda base de datos.
2.7.5.7 Destrucción de la base de datos, que destruye permanentemente el vídeo más antiguo que el límite máximo de días de grabación.

2.8 Sincronización horaria

2.8.1 Todo el sistema deberá poder sincronizarse en el tiempo utilizando el Protocolo de Tiempo de Red (NTP).

2.9 Ciberseguridad

2.9.1 El sistema debe garantizar una comunicación segura entre los componentes del VMS, incluyendo:

- 2.9.1.1 Servidores de grabación a clientes.
- 2.9.1.2 Servidores de grabación a otros servidores de grabación.
- 2.9.1.3 Servidores de grabación a Video Walls.
- 2.9.1.4 Servidores de grabación al portal de gestión de alarmas.

2.9.2 Las siguientes medidas de seguridad se emplean durante la comunicación entre los componentes del VMS:

- 2.9.2.1 El motor de cifrado utilizará openssl (hashes SHA512, DH-RSA efímero con forward secrecy [DH 2048 bits] y cifrados simétricos AES-GCM de 128 bits) equivalente a TLS 1.3.
- 2.9.2.2 Las contraseñas nunca se almacenan como texto sin formato, sino que se etiquetan con SHA512.
- 2.9.2.3 Las credenciales de acceso se negocian utilizando RSA1024.
- 2.9.2.4 Los canales de comunicación confidencial son encriptados usando AES128/CBC.
- 2.9.2.5 Se utiliza HMAC para la verificación de la integridad.
- 2.9.2.6 Todas las conexiones externas del sitio soportan varios niveles de encriptación:
  - 2.9.2.6.1 Desactivado.
  - 2.9.2.6.2 Mínimo - sólo se cifrarán las conexiones críticas.
  - 2.9.2.6.3 Seguro (por defecto) - todas las conexiones, excepto las de alto volumen de vídeo, deben ser encriptadas.
  - 2.9.2.6.4 Todo - todas las conexiones, incluyendo las de alto volumen de vídeo, deberán estar encriptadas.
- 2.9.2.7 La infraestructura de clave pública (PKI) es gestionada internamente por el VMS para mayor seguridad.

2.9.3 El sistema deberá garantizar la seguridad e integridad del vídeo grabado a través de los siguientes medios:

- 2.9.3.1 Se utilizan claves dobles RSA1024 (para la firma) para asegurar la integridad del vídeo que se exporta/archiva.
- 2.9.3.2 El cifrado opcional utiliza el cifrado de bloques AES128 con un IV aleatorio por bloque y una frase de contraseña generada por el usuario.
- 2.9.3.3 El vídeo archivado puede llevar una marca de agua para indicar la fuente de la información (es decir, información del usuario).
- 2.9.3.4 Las secuencias de vídeo archivadas y los metadatos están restringidos a la reproducción a través del reproductor de vídeo propietario del VMS.
- 2.9.3.5 El vídeo exportado/archivado puede estar restringido a una reproducción controlada por contraseña.

2.9.4 El sistema deberá, en cuanto a que estas medidas sean admitidas por los fabricantes, garantizar la seguridad de las cámaras IP conectadas por los siguientes medios:

2.9.4.1 Conexión segura de la cámara:

2.9.4.1.1 HTTP: protocolo de transferencia de hipertexto.

2.9.4.1.2 Conexiones de control cifradas HTTPS.

2.9.4.1.3 SSL/TLS cifrado.

2.9.4.1.4 Soporte de CURL (biblioteca de transferencia de URL del lado del cliente).

2.9.4.2 Control seguro de la cámara:

2.9.4.2.1 RTSP - protocolo de transmisión en tiempo real.

2.9.4.2.2 Control cifrado HTTPS.

2.9.4.3 Transmisión segura de vídeo:

2.9.4.3.1 RTP - control de transporte en tiempo real.

2.9.4.3.2 Vídeo encriptado.

3 Requisitos del software de gestión de vídeo (VMS)

3.1 Soporte de cámaras IP

3.1.1 El VMS deberá soportar tanto Onvif-S como interfaces de cámara nativas.
3.1.2 El VMS deberá soportar cámaras IP multicabezales.
3.1.3 El VMS deberá soportar codificadores de vídeo.
3.1.4 El VMS deberá soportar los protocolos de cámara MJPEG, H.264, H.265 y MxPEG.
3.1.5 La interfaz entre el VMS y la cámara deberá ser UPnP (universal plug and play), si la cámara lo admite.
3.1.6 El VMS deberá soportar flujos de vídeo de velocidad de bits variable y fija.
3.1.7 El VMS deberá soportar múltiples flujos de vídeo y resoluciones de vídeo, limitados únicamente por las propias cámaras integradas.
3.1.8 El VMS deberá admitir cámaras de 360 y 180 grados, y disponer de un software integrado que pueda desenfocar dichas cámaras.
3.1.9 El VMS debe ser compatible con las cámaras PTZ:

3.1.9.1 El VMS deberá tener la capacidad de programar posiciones preestablecidas de cámaras PTZ y asignar nombres únicos a cada posición preestablecida.
3.1.9.2 El VMS deberá admitir las funciones de zoom de área en las cámaras seleccionadas, lo que permitirá a la cámara desplazarse y hacer zoom en un área seleccionada por el usuario.
3.1.9.3 La prioridad de control de PTZ se asignará en función de la jerarquía de los derechos de acceso.

3.1.10 El VMS sólo ofrecerá los ajustes de la cámara que estén disponibles en la cámara específica.
3.1.11 El VMS deberá soportar las entradas y salidas de la cámara.
3.1.12 El VMS deberá soportar el audio sincronizado de la cámara.
3.1.13 El VMS deberá soportar el audio bidireccional.
3.1.14 El VMS deberá ser capaz de recibir eventos analíticos de las cámaras seleccionadas que ofrezcan esta capacidad.
3.1.15 El VMS deberá permitir al usuario "navegar" directamente a la URL de la cámara o a la página web desde la ventana de configuración de la cámara.
3.1.16 La cámara deberá poder configurarse como cámara "encubierta".
3.1.17 El VMS deberá admitir zonas de privacidad, que permitan al usuario definir las áreas que se ocultarán de la vista del operador.

3.2 Interfaz gráfica de usuario

3.2.1 El VMS deberá soportar la traducción de la Interfaz Gráfica de Usuario (GUI) a múltiples idiomas, incluyendo:

3.2.1.1 Árabe.
3.2.1.2 Holandés.
3.2.1.3 Inglés.
3.2.1.4 Francés.
3.2.1.5 Húngaro.
3.2.1.6 Italiano.
3.2.1.7 Portugués.
3.2.1.8 Español.

3.2.2 El VMS deberá permitir la grabación de las cámaras en las bases de datos definidas por el usuario.
3.2.3 El VMS deberá proporcionar opciones de grabación configurables antes y después de los eventos.
3.2.4 El VMS deberá proporcionar un verdadero entorno "triplex", permitiendo la grabación, la visualización en vivo y la reproducción simultánea en múltiples cámaras.
3.2.5 El VMS debe permitir a los usuarios definir múltiples bases de datos y seleccionar a qué base de datos debe grabar cada cámara.
3.2.6 El VMS deberá permitir la grabación tanto de vídeo como de audio.
3.2.7 El VMS deberá permitir el inicio de la grabación a través de uno de los siguientes métodos:

3.2.7.1 Continuo.
3.2.7.2 Horario programado.
3.2.7.3 Tras un evento.
3.2.7.4 Por iniciativa del usuario.

3.2.8 Los usuarios deben poder elegir qué flujo de vídeo de las cámaras seleccionadas quieren grabar.
3.2.9 El VMS deberá permitir la grabación de una cámara en múltiples bases de datos simultáneamente.
3.2.10 El VMS debe permitir al usuario ver de 1 a 64 cámaras en una pantalla en diseños definidos por el usuario.
3.2.11 El VMS debe proporcionar la capacidad de realizar recorridos por los diseños en los monitores de Video Wall.
3.2.12 El VMS debe proporcionar un Panel Mímico para el control de múltiples monitores en un Video Wall.
3.2.13 El sistema deberá proporcionar una capacidad de mapeo de cámaras adyacentes, que proporcione la facilidad de vincular cámaras geográficamente próximas en el software, y poder navegar fácilmente entre las cámaras vinculadas en la interfaz del operador para seguir objetos/sospechosos que se muevan a través de múltiples cámaras.
3.2.14 El Seguimiento de Sospechosos pretende vincular la función de mapeo de cámaras adyacentes a un uso de seguridad deseado.
3.2.15 El VMS debe permitir a los usuarios crear diseños de pantalla y guardarlos con nombres definidos por el usuario.
3.2.16 Los diseños definidos por el usuario se mostrarán como iconos en el panel de recursos y el usuario podrá recuperarlos fácilmente.
3.2.17 El VMS deberá permitir a los usuarios hacer zoom digitalmente en la vista de la cámara utilizando la rueda de desplazamiento del ratón.
3.2.18 El VMS debe proporcionar la capacidad de realizar recorridos de cámara (secuencias) dentro de un panel de cámara o en un monitor seleccionado con retrasos de tiempo configurables entre cada secuencia de cámara. Esto se hará mediante la presentación de flechas superpuestas que indiquen la dirección en la siguiente cámara próxima.
3.2.19 El sistema deberá permitir al usuario marcar disposiciones de cámara favoritas en directo/revisión sólo para los recursos a los que el usuario tenga derechos de acceso.
3.2.20 El sistema deberá proporcionar un sistema de gestión de imágenes de referencia que cree imágenes de referencia con marca de tiempo de la orientación de todas las cámaras del servidor.

3.2.20.1 El sistema deberá permitir la comparación entre las imágenes de referencia capturadas y la imagen actual (no capturada) del servidor.

3.2.20.2 El sistema deberá mostrar el porcentaje de diferencia entre las dos imágenes comparadas.

3.2.21 Si se han configurado múltiples flujos de vídeo en la cámara para su visualización en directo, el usuario deberá poder elegir qué flujo de vídeo desea ver. Esto permite a los usuarios ver resoluciones más bajas para el monitoreo fuera del sitio.

3.2.22 El VMS deberá contar con un sistema de gestión de derechos de acceso de varios niveles.

3.2.23 El VMS deberá permitir al administrador asignar características y funciones a niveles de usuario seleccionados.

3.2.24 El VMS deberá ser compatible con LDAP, OpenLDAP y Windows Active Directory.

3.2.25 El sistema deberá proporcionar registros de auditoría con registros completos de todas las actividades de los usuarios.

3.2.26 El sistema deberá permitir a los administradores filtrar los registros de auditoría por lo siguiente:

3.2.26.1 Hora.

3.2.26.2 Periodo de tiempo.

3.2.26.3 Identificación del usuario.

3.2.26.4 Recursos (por ejemplo, cámaras).

3.2.26.5 Acciones del usuario.

3.2.27 El VMS deberá permitir la exportación de los registros de auditoría en formato de archivo CSV.

3.2.28 El VMS debe permitir a los usuarios con derechos de acceso la capacidad de archivar (exportar) el vídeo seleccionado a una carpeta seleccionada o a un medio de almacenamiento externo.

3.2.29 Para garantizar la seguridad del vídeo, el vídeo exportado se "firmará" digitalmente utilizando claves RSA1024 y el cifrado opcional se realizará mediante el cifrado de bloques AES128 con un IV aleatorio por bloque y una frase de paso generada por el usuario.

3.2.30 El VMS deberá contar con lo siguiente para la protección de la privacidad del vídeo archivado (exportado):

3.2.30.1 Una marca de agua definida por el usuario.

3.2.30.2 Una contraseña definida por el usuario, que debe introducirse antes de poder reproducir el vídeo exportado.

3.2.31 El VMS debe permitir al usuario revisar las grabaciones de varias cámaras simultáneamente.

3.2.32 El VMS debe permitir al usuario revisar las grabaciones de las cámaras compatibles con Edge.

3.2.33 El VMS debe permitir a los usuarios sincronizar la reproducción de varias cámaras.

3.2.34 El VMS deberá proporcionar funciones de búsqueda avanzada para que los usuarios puedan encontrar las secuencias de vídeo pertinentes de manera eficiente, como se indica a continuación:

3.2.34.1 Línea de tiempo:

3.2.34.1.1 El VMS deberá permitir a los usuarios navegar hasta las secuencias grabadas arrastrando la barra de la línea de tiempo.

3.2.34.1.2 El VMS debe permitir a los usuarios navegar hasta las secuencias grabadas seleccionando una fecha y hora en el calendario.

3.2.34.1.3 El usuario deberá poder hacer "zoom" en la barra de la línea de tiempo utilizando la rueda de desplazamiento del ratón.

3.2.34.2 Búsqueda de movimiento:

3.2.34.2.1 El VMS deberá contener una función de Búsqueda de Movimiento que permita al usuario encontrar un vídeo seleccionando un área dentro de la vista de la cámara y realizando la búsqueda.

3.2.34.2.2 Esta función utilizará los metadatos de movimiento de vídeo almacenados en el servidor para realizar esta búsqueda.

3.2.34.2.3 Cualquier movimiento que se descubra dentro de esta zona se mostrará en la barra de la línea de tiempo de la interfaz de usuario.

3.2.34.3 Búsqueda instantánea (Snapshot Search):

3.2.34.3.1 El VMS contendrá una función de Búsqueda de Instantáneas, que permite a los usuarios ver instantáneas divididas a lo largo de un tiempo seleccionado para encontrar fácilmente los incidentes que hayan ocurrido.

3.2.34.3.2 La función deberá permitir a los usuarios reducir fácilmente el lapso de tiempo (drilling-down) arrastrando entre dos instantáneas.

3.2.34.3.3 El usuario deberá poder reproducir las imágenes grabadas desde la hora de la instantánea elegida, directamente desde la ventana de búsqueda de instantáneas.

3.2.34.4 Superposición de rutas de actividad:

3.2.34.4.1 El VMS deberá proporcionar una superposición de movimiento de vídeo pasado a petición.

3.2.34.4.2 El usuario deberá ser capaz de reproducir inmediatamente el vídeo del tiempo de superposición seleccionado utilizando los comandos del ratón.

3.2.34.5 Mapas de calor:

3.2.34.5.1 El sistema deberá ser capaz de mostrar una superposición de mapas de calor para indicar las áreas de movimiento en una imagen de cámara.

3.2.34.5.2 El sistema deberá ser capaz de refinar los resultados de los mapas de calor mediante el análisis de períodos.

3.2.35 El VMS deberá ofrecer las siguientes funciones de gestión de eventos:

3.2.35.1 Los eventos pueden ser activados por:

3.2.35.1.1 Disparos de análisis de vídeo desde el análisis de a bordo o el análisis de Edge (dependiendo de la cámara).

3.2.35.1.2 Entradas de E/S de la cámara u otras entradas de E/S.

3.2.35.1.3 Activadores iniciados por el usuario.

3.2.35.1.4 Activadores de eventos de terceros (por ejemplo, control de acceso, paneles de intrusión/incendio).

3.2.35.1.5 Alarmas técnicas:

3.2.35.1.5.1 Manipulación de la cámara.
3.2.35.1.5.2 Fallo de la cámara.
3.2.35.1.5.3 Fallo del disco duro.
3.2.35.1.5.4 Errores de la base de datos.
3.2.35.1.5.5 Fallo del sistema.
3.2.35.1.5.6 Errores del servidor de software.
3.2.35.1.5.7 Alarma de conectividad de red.
3.2.35.1.5.8 Alarmas de reinicio del sistema.
3.2.35.1.5.9 Alarma de archivo programado.
3.2.35.1.6 Alarma de prueba.
3.2.35.2 Las acciones de los eventos deben incluir:
3.2.35.2.1 Grabación de un flujo de vídeo seleccionado por la cámara en una base de datos seleccionada.
3.2.35.2.2 Conmutación de una cámara a un monitor de video wall seleccionado o a un monitor local.
3.2.35.2.3 Reproducir un clip de audio seleccionado a:
3.2.35.2.3.1 Salida de audio del servidor de cliente.
3.2.35.2.3.2 Salida de audio de la cámara.
3.2.35.2.4 Envío de una alarma al portal de gestión de alarmas.
3.2.35.2.5 Envío de una alarma a una interfaz cliente-servidor.
3.2.35.2.6 Envío de un correo electrónico.
3.2.35.2.7 Envío de un SMS.
3.2.35.2.8 Mover una cámara PTZ a una posición preestablecida.
3.2.36 El VMS debe ser compatible con los clientes móviles IOS y Android.
3.2.37 El VMS debe ser capaz de mostrar superposiciones de texto en la transmisión de vídeo desde dispositivos de terceros.
3.2.38 El VMS debe tener la capacidad de integrarse con los sistemas de terceros como el control de acceso, alarmas de intrusión y paneles de fuego para proporcionar la siguiente funcionalidad:

3.2.38.1 Recepción de datos/mensajes de eventos de sistemas de terceros.
3.2.38.2 Asociar una o más cámaras con dispositivos específicos de sistemas de terceros.
3.2.38.3 Almacenamiento de datos de sistemas de terceros junto con el vídeo asociado en bases de datos seleccionadas.
3.2.38.4 Visualización de superposiciones de datos de sistemas de terceros en la vista en directo.
3.2.38.5 Permitir la extracción de datos de la base de datos de integración de terceros para encontrar fácilmente las transacciones y las secuencias de vídeo asociadas.
3.2.39 El VMS deberá ser capaz de conectarse con teclados/joysticks del proveedor o de terceros.
3.2.40 El VMS deberá proporcionar una función de mapa jerárquico que permita al usuario:

3.2.40.1 Crear mapas utilizando archivos JPG o PNG.
3.2.40.2 Añadir cámaras u otros recursos desde el editor de mapas.
3.2.40.3 Crear polígonos que puedan mostrar acciones definidas por el usuario y "pop-up" en eventos.
3.2.40.4 Crear iconos de activación del usuario.

3.2.40.5 Crear áreas de preajuste PTZ que, al hacer clic, moverán automáticamente la cámara PTZ a la posición asociada.
3.2.40.6 Desglosar varias capas del mapa desde la interfaz de usuario.
3.2.40.7 Conectarse automáticamente a un sitio remoto desde la interfaz del mapa.
3.2.41 El VMS debe proporcionar una infraestructura para informar sobre la supervisión de la condición y el estado del sistema:

3.2.41.1 Fallos de la cámara, registros, estado y tiempo de reparación.
3.2.41.2 Uso de la base de datos:
3.2.41.2.1 Desglose por cámara.
3.2.41.2.2 Velocidad por cámara/hora/cámara por hora.
3.2.41.3 Histograma de frecuencia de eventos.
3.2.41.4 Eventos por hora.
3.2.41.5 Disco.
3.2.41.6 Eventos.
3.2.41.7 Sistemas de archivos.
3.2.41.8 Hardware.
3.2.41.9 Licencias.
3.2.41.10 Consultas de protocolo de tiempo de red.
3.2.41.11 Reinicios y causas de reinicios, incluyendo:
3.2.41.11.1 Reinicios del servidor de software.
3.2.41.11.2 Reinicios por fallo de alimentación.
3.2.41.11.3 Reinicios de usuario.
3.2.41.11.4 Reinicios de usuarios remotos.
3.2.41.11.5 Hora de reinicio.
3.2.41.12 Instalación y configuración de la grabación, tiempos (del sistema por cámara) y fallos de grabación.
3.2.41.13 Instalación y configuración del sistema.
3.2.41.14 Fallos del servidor de software.
3.2.41.15 Tiempo de funcionamiento de la unidad.
3.2.41.16 Informes de cámaras con fallos actuales.
3.2.41.17 Alertas de condición en la barra de estado. Se mostrará un mensaje si el disco en el que está instalado el NVR se está llenando.

3.3 Failover

3.3.1 El sistema deberá soportar la Failover de los servidores n:1 y n:n.
3.3.2 Un servidor de Failover deberá ser un "hotspare" y asumir las funciones de cualquier servidor que falle, incluido el servidor maestro.
3.3.3 La Failover incluirá todas las funciones del servidor de grabación.
3.3.4 La Failover incluirá todas las funciones de gestión del Video Wall.
3.3.5 La Failover incluirá todas las funciones de gestión de eventos y acciones.
3.3.6 Cuando se produzca un fallo en el sistema, el servidor de Failover deberá grabar las secuencias de vídeo en una base de datos específica.
3.3.7 Cuando se sustituya un servidor que haya fallado, las secuencias de vídeo de la base de datos de Failover se reintroducirán automáticamente en la base de datos original.

3.4 Teclado/Controlador

3.4.1 El sistema deberá contar con un teclado/controlador integrado.
3.4.2 El sistema deberá permitir la configuración de la sensibilidad PTZ en el software.
3.4.3 El teclado deberá permitir la selección rápida de cámaras, preajustes, monitores, salidas, recorridos de cámara (secuencias) y diseños de pantalla.
3.4.4 Los botones de función de la cámara PTZ deberán ser accesibles a los dedos de la mano del joystick, para que los operadores no tengan que renunciar al control del mismo.
3.4.5 La pantalla LCD del teclado deberá poder ser escrita por el sistema de vigilancia digital.
3.4.6 Los LED del teclado deberán indicar el estado de las teclas y las funciones.

3.5 Análisis de vídeo

3.5.1 El VMS deberá proporcionar análisis de vídeo integrados y patentados, disponibles bajo licencia, como se indica a continuación:

3.5.1.1 Detección básica de movimiento en vídeo.
3.5.1.2 Detección avanzada de movimiento por vídeo con modelado dinámico del fondo y algoritmos de aprendizaje.
3.5.1.3 Movimiento en el área.
3.5.1.4 Ausencia de movimiento en un área donde se espera que haya movimiento.
3.5.1.5 Grabación de movimiento simple.
3.5.1.6 Cruce de líneas de objetos.
3.5.1.7 Dirección del objeto.
3.5.1.8 Velocidad del objeto.
3.5.1.9 Merodeo de objetos.
3.5.1.10 Entrada del objeto en la zona.
3.5.1.11 Objeto que sale del área.
3.5.1.12 Clasificación de objetos.
3.5.1.12.1 El sistema deberá contar con una base de datos de clasificación de objetos para almacenar las clasificaciones de los mismos.
3.5.1.13 Detección de objetos a la izquierda.
3.5.1.14 Manipulación de la cámara.
3.5.1.15 Recuento de objetos.

3.5.2 La interfaz de usuario del VMS debe proporcionar superposiciones de análisis de vídeo para mostrar lo siguiente:

3.5.2.1 Actividad de análisis de vídeo.
3.5.2.2 Activadores de análisis de vídeo.
3.5.2.3 Zonas de análisis de vídeo.

3.5.3 Los algoritmos de análisis de vídeo deberán ser capaces de iniciar eventos únicos dentro del software VMS

3.6 Reconocimiento automático de matrículas (ANPR)

3.6.1 El sistema ANPR deberá proporcionar la capacidad de reconocer las matrículas por región y tener la siguiente capacidad:

3.6.1.1 La solución ANPR deberá funcionar con cualquier cámara IP adecuada o con una resolución, frecuencia de imagen y velocidad de obturación adecuadas con una iluminación apropiada.

3.6.2 La capacidad de configuración debe incluir:

3.6.2.1 Ajuste de la inclinación.
3.6.2.2 Ajuste del área de identificación.
3.6.2.3 Ajuste del tamaño previsto de los caracteres de la matrícula.
3.6.2.4 Prueba del metraje de grabación.

3.6.3 Las superposiciones de información sobre las matrículas se mostrarán en el vídeo en directo y/o grabado e incluirán:

3.6.3.1 Datos de la matrícula.
3.6.3.2 Fotografía de la matrícula.

3.6.4 El sistema deberá incluir la capacidad de agrupar los datos de las matrículas en categorías específicas definidas por el usuario, tales como visitantes, personal, lista blanca, lista negra, etc.

3.6.5 El sistema deberá proporcionar la capacidad de crear reglas de eventos/alarmas si se detecta una matrícula de un grupo seleccionado (por ejemplo, si se detecta una matrícula del grupo de personal, se puede desear abrir automáticamente una barrera. Si se detecta una matrícula de un grupo de la lista negra, se puede querer activar una alarma).

3.6.6 El sistema deberá permitir importar la información de las matrículas para incluirlas en los grupos seleccionados (por ejemplo, personal, lista negra).

3.6.7 El sistema deberá permitir al usuario añadir información personalizada a las matrículas conocidas. Por ejemplo, el tipo de vehículo, el nombre de la persona, etc.

3.6.8 El sistema deberá ser capaz de filtrar la base de datos ANPR por un número de opciones, incluyendo entre otros, lo siguiente:

3.6.8.1 Hora/fecha.
3.6.8.2 Matrículas/Grupos.
3.6.8.3 Confianza (precisión de la captura de matrículas en porcentaje).
3.6.8.4 Detector ANPR.
3.6.8.5 Cámara.
3.6.8.6 Nombre del conductor/empresa.
3.6.8.7 Tipo/marca/modelo/color del vehículo.
3.6.8.8 Lugar de emisión (específico de la región).
3.6.8.9 Color de fondo, color del texto y forma de la matrícula.
3.6.8.10 Posición de la matrícula en el coche (delante/detrás).
3.6.8.11 Posición del coche en el carril (entrada/salida).
3.6.8.12 Informes ANPR basados en filtros.

3.7 Portal de gestión de alarmas

3.7.1 El sistema deberá proporcionar un sistema centralizado de gestión de alarmas/eventos que permita la gestión de eventos y/o alarmas desde el sitio local o desde múltiples sitios remotos.

3.7.2 El sistema de gestión de alarmas deberá supervisar las conexiones con las unidades remotas a través de un latido del sitio a intervalos establecidos. Generará un disparo cuando una unidad de alarma remota no envíe su latido.

3.7.3 La interfaz de la alarma deberá tener un control de acceso, independiente del resto del software, y deberá tener su propia utilidad de gestión de usuarios.

3.7.4 El sistema mostrará las alarmas en paneles separados según su estado:

3.7.4.1 Entrante (a la espera de ser atendida por un operador).
3.7.4.2 En curso (siendo atendida por un operador).
3.7.4.3 Archivada (ya tratada por un operador).

3.7.5 El sistema deberá permitir la personalización de las notificaciones de audio de las alarmas entrantes.

3.7.6 El sistema deberá mostrar las alarmas según su prioridad, indicada por diferentes colores, tal y como se ha configurado para las alarmas de eventos.

3.7.7 El sistema deberá tener la capacidad de reproducir las alarmas de audio según el nivel de prioridad de la alarma.

3.7.8 En caso de que varios operadores manejen las alarmas, el sistema deberá mantener a todos los operadores informados sobre el estado de una alarma y sobre quién la maneja.

3.7.9 El sistema deberá permitir a los operadores responder a una alarma y:

3.7.9.1 Conectarse automáticamente al sitio desde donde se inició la alarma.
3.7.9.2 Mostrar automáticamente el mapa del sitio desde donde se inició la alarma.

3.7.10 El sistema deberá ser capaz de deshabilitar temporalmente (bloquear) las alarmas inválidas repetitivas durante períodos especificados. Este bloqueo se especificará desde la unidad del portal, y requerirá un comentario explicativo por parte del operador del bloqueo.

3.7.11 El sistema deberá permitir a los operadores borrar simultáneamente varias alarmas de la cola de entrada.

3.7.12 El sistema deberá permitir a los operadores añadir comentarios a las alarmas actuales y archivadas. Para facilitar una respuesta rápida, los comentarios predeterminados se podrán seleccionar en un menú, pero también será posible añadir comentarios de texto personalizados.

3.7.13 El sistema deberá permitir a los operadores modificar el menú de comentarios por defecto con comentarios personalizados más adecuados.

3.7.14 El sistema deberá permitir a los operadores escalar electrónicamente una alarma a un "caso", y asignar personas para investigar, alertando e involucrando así a las estructuras de gestión de la seguridad.

3.7.15 El sistema deberá permitir a los operadores filtrar las alarmas históricas utilizando sus grabaciones y metadatos asociados. Los parámetros de filtrado deberán incluir:

3.7.15.1 Alarmas, Sesiones (donde se pueden haber enviado múltiples alarmas en una sola conexión).
3.7.15.2 Operador de la sala de control (basado en la información de inicio de sesión).
3.7.15.3 Casos (alarmas que se han escalado para una mayor investigación).

3.7.16 El sistema deberá permitir a los operadores hacer doble clic en una entrada (alarma, sesión, inicio de sesión del operador, caso) de la interfaz de alarmas históricas, para mostrar una pantalla de información/acción más detallada relacionada con esa entrada, desde la cual será posible hacer lo siguiente:

3.7.16.1 Ver el nombre del sitio de la alarma.
3.7.16.2 Ver el nombre del servidor de alarmas.
3.7.16.3 Ver la descripción de la alarma.
3.7.16.4 Ver el operador de la sala de control que manejó una alarma o una sesión.
3.7.16.5 Ver el nombre de la unidad de la sala de control a través de la cual se gestionó una alarma o una sesión.
3.7.16.6 Ver la hora de un evento de alarma.

3.7.16.7 Ver la hora en que se envió un evento de alarma a la sala de control.
3.7.16.8 Ver la hora de llegada de una alarma a la sala de control.
3.7.16.9 Ver el tiempo que tarda el operador de la sala de control en gestionar una alarma.
3.7.16.10 Ver los comentarios asociados a las alarmas, sesiones y casos.
3.7.16.11 Ver las grabaciones asociadas a una alarma.
3.7.16.12 Conectar con el sitio histórico de la alarma para obtener más grabaciones asociadas a la alarma, si todavía existen en la base de datos del sitio remoto.
3.7.16.13 Ver los casos asociados a una alarma.
3.7.16.14 Mostrar toda la sesión en la que se ha gestionado una alarma.
3.7.16.15 Añadir más comentarios a las alarmas, sesiones y casos históricos.
3.7.16.16 Escalar una alarma histórica a un Caso para una mayor investigación y resolución.
3.7.16.17 Mostrar los inicios de sesión del operador de la sala de control asociados a una sesión de alarma.
3.7.16.18 Ver todas las alarmas asociadas a una sesión.
3.7.16.19 Ver la duración del inicio de sesión del operador de la sala de control, la hora de inicio y la hora de finalización.
3.7.16.20 Ver el número de sesiones gestionadas por un operador de sala de control durante un inicio de sesión.
3.7.16.21 Ver todas las sesiones gestionadas por un operador de la sala de control durante un inicio de sesión.
3.7.16.22 Ver la descripción de un caso.
3.7.16.23 Ver el nombre del usuario que escaló una alarma a un caso, con la fecha-hora.
3.7.16.24 Ver el nombre del usuario que cerró un Caso, con la fecha-hora.
3.7.16.25 Ver una lista de usuarios de Casos, con su Estado relacionado con un Caso (Activo - aún trabajando en él, o Inactivo - ya no trabajando en él).
3.7.16.26 Ver una línea de tiempo de las acciones de los usuarios relacionadas con un caso.
3.7.16.27 Ver el estado de un caso.
3.7.16.28 Ver todas las alarmas asociadas a un caso.
3.7.16.29 Ver todos los comentarios asociados a un caso
3.7.17 El sistema deberá proporcionar informes que puedan ser personalizados para adaptarse a las necesidades de los clientes.

3.8 Interfaz de programación de aplicaciones

3.8.1 El sistema deberá incluir una interfaz de programación de aplicaciones (API) que permita a los programas informáticos de terceros recuperar y gestionar la información del sistema de gestión de vehículos, así como controlar los recursos del sistema.
3.8.2 El sistema deberá restringir el acceso al sitio a través de la autenticación digital y en base a los niveles de acceso preconfigurados del usuario.
3.8.3 El sistema deberá proporcionar la capacidad de hacer una lista de todas las cámaras y recursos de cámaras en un sitio. Nota: las fuentes con formatos de vídeo no compatibles con RTSP se excluirán de la lista de cámaras de la API.
3.8.4 El sistema deberá incluir información de identificación de la alimentación de la cámara, como el nombre, el ID único, la alimentación de audio (sí/no), la información del nivel de acceso, el estado "en línea/fuera de línea" de la cámara, el estado de PTZ, la información de patrones/preajustes y la información de la pista de vídeo en directo y de revisión.

3.8.5 El sistema debe permitir la transmisión de vídeo en directo y de revisión de la cámara mediante el protocolo RTSP.

3.8.6 El sistema requerirá la autenticación del cliente para la transmisión de vídeo en directo.

3.8.7 El sistema deberá ser compatible con los siguientes transportes de transmisión:

3.8.7.1 RTP sobre UDP.

3.8.7.2 RTP sobre TCP.

3.8.8 El sistema deberá permitir la transmisión de entradas y salidas de audio independientes hacia y desde las entradas y salidas de audio del servidor a través del protocolo SIP.

3.8.9 El sistema deberá permitir el control de las cámaras PTZ.

3.8.10 El sistema deberá supervisar y actualizar, a petición, todas las E/S actuales del sitio.

3.8.11 El sistema deberá ser capaz de recibir alarmas técnicas y de eventos desde el servidor.

3.8.12 El sistema deberá tener una interfaz de línea de tiempo.