DOCUMENTO TÉCNICO

Protección perimetral para aeropuertos con videovigilancia inteligente

Reflexiones sobre el servicio prestado y el rendimiento de la inversión

Abril 2024

AXIS COMMUNICATIONS

Resumen

La protección perimetral tradicional de los aeropuertos suele consistir en vallas o muros, que delimitan el perímetro e impiden el acceso de intrusos. El perímetro también debe contar con un sistema de detección de intrusos que envíe las alarmas a una estación de supervisión. Las soluciones disponibles para la detección en el perímetro y alrededor de este pueden ser, por ejemplo, detectores con cables, sensores de microondas o cables de traspaso infrarrojos. Aunque son útiles, ninguno de estos métodos resulta infalible. Las detecciones fallidas son un problema, y otro, igual de problemático, son los falsos positivos, que a la larga pueden hacer que se omitan por completo incidentes potencialmente graves.

La combinación de cámaras de videovigilancia y software de detección de movimiento y basado en la IA ha ampliado el rango y las prestaciones de las soluciones de protección perimetral, desde la simple detección hasta el análisis complejo de los accesos no autorizados. Según la legislación local, la tecnología de las cámaras puede utilizarse para supervisar más allá del perímetro físico, proporcionando un margen de vigilancia adicional y brindando al operador un tiempo extra para poder responder.

La tecnología de sensores térmicos ha mejorado de manera significativa en los últimos años, y los costes asociados han disminuido. Las cámaras térmicas, junto con el software de analítica de vídeo, pueden proteger una zona en cualquier momento del día, independientemente de las condiciones de iluminación. La tecnología térmica suele ser muy adecuada para los aeropuertos, puesto que ofrece una excelente capacidad de detección en grandes instalaciones.

Cuando no existe la posibilidad de usar la tecnología térmica, la tecnología de microondas (radar) puede representar una excelente alternativa, dado que ofrece muchas de las mismas ventajas. El radar de Axis puede diferenciar los objetivos e integrarse con las cámaras PTZ para realizar un seguimiento eficaz de un objetivo. Esta tecnología funciona las 24 horas del día sin interrupción con un número mínimo de falsos positivos, lo que supone un ahorro debido a los bajos costes de investigación, así como a la existencia de un equipo de seguridad más reducido que puede centrarse en las amenazas reales.

La evaluación de una solución de protección perimetral debe ser adecuada y proporcionada. Atajar las amenazas es siempre el principal aspecto a tener en cuenta, pero al mismo tiempo el sistema debe cumplir con todos los requisitos legales.

Demostrar el rendimiento de la inversión de una solución de seguridad suele ser difícil, al no haber ingresos que se puedan comparar con el coste. Sin embargo, el uso de tecnología que reduce la necesidad de llevar a cabo intervenciones manuales puede proporcionar resultados más tangibles. Las cámaras también pueden utilizarse para elevar la eficiencia, por ejemplo, utilizando una pantalla para mostrar a los intrusos que se han grabado datos que les identifican.

Las cámaras Axis están equipadas con funciones sofisticadas para obtener imágenes de más calidad, una mejor conectividad del hardware y una compresión superior. También cuentan con nuestros propios procesadores ARTPEC, que permiten integrar soluciones de analítica de vídeo para protección perimetral en el extremo. Esta arquitectura técnica distribuida permite añadir más cámaras según sea necesario, y al mismo tiempo prescinde de las inversiones en tecnología de servidores centralizados.

Índice

1 Introducción

La seguridad de una instalación crítica se basa en dos pilares: el diseño y la protección. Los aeropuertos suelen considerarse parte de las infraestructuras críticas de un país y se les exige que limiten los riesgos de acceso de intrusos mediante la aplicación de soluciones de seguridad adecuadas, a menudo como parte de una estrategia estructurada y por niveles que incluye barreras físicas, detección de intrusos, control de acceso y patrullas de seguridad móviles.

Evidentemente, las medidas adoptadas para proteger las zonas restringidas de un aeropuerto deben tener en cuenta tanto la amenaza como los requisitos operativos, en concreto las servidumbres de aviación, la topografía del terreno, las condiciones climáticas específicas y las limitaciones medioambientales. En este documento técnico se pretende explicar algunas de las opciones actuales para proteger los aeropuertos y se ofrece información sobre la tecnología que hay detrás de las soluciones.

2 Soluciones de protección perimetral tradicionales

2.1 Soluciones físicas

Las soluciones físicas suelen ser un componente fundamental del «nivel exterior» de un enfoque compartimentado de la seguridad de una instalación, que suele consistir en una valla perimetral, a menudo construida con malla metálica o soldada, en paneles soldados o de hormigón. En las zonas próximas a equipos de radionavegación y comunicaciones, se utilizan vallas no magnéticas. Estas vallas tienen varios cometidos: son una forma de definir claramente los límites del aeropuerto, pero también disuaden de la entrada de personas y animales. También se pueden añadir elementos como sistemas antiescalada, vías de acceso de vehículos, sistemas de disuasión de entrada, cimientos y paneles de vallas.

Para mejorar la seguridad, el perímetro debe contar con soluciones automáticas de detección de intrusos, que envían una alarma a una estación de supervisión para que se investiguen las posibles vulneraciones de acceso.

2.2 Detección de intrusos en vallas y puertas de acceso

Existen diferentes tipos de «detectores» mediante cables para proteger perímetros extensos; esos sistemas redirigen las alarmas en tiempo real a un operador de seguridad. Algunos proveedores ofrecen vallas provistas de soluciones de detección automática.

Estas soluciones, al igual que la videovigilancia o cualquier otra solución, no son infalibles y pueden generar falsas alarmas, que reciben el nombre de «falsos positivos». Algunas de las causas habituales de los falsos positivos son los animales, el balanceo de los árboles y las condiciones meteorológicas adversas. Sin videovigilancia, la única forma de verificar qué ha causado la alarma es enviar personal a investigar. La reiteración de falsos positivos puede ocasionar apatía entre el personal, lo que a su vez puede dar lugar a que se haga caso omiso de las alertas y, en última instancia, se pase por alto una amenaza real.

2.3 Detectores de intrusos fuera de las vallas

Otros detectores de intrusos, como los sensores de microondas, las barreras de infrarrojos o los láseres, se colocan en lugares estratégicos del perímetro del aeropuerto. Una vez más, estos sistemas pueden verse limitados por aspectos como los falsos positivos y la capacidad de detección limitada de distancia y altura si no se siguen estrictamente las normas de instalación. El uso de radares (microondas) en el

perímetro puede resultar problemático en un entorno de aviación, puesto que los dispositivos interfieren con la tecnología existente en el mismo espectro y podrían descartarse únicamente por esta razón. Los posibles problemas que plantean estos dispositivos pueden desaparecer casi por completo si se elige cuidadosamente la frecuencia y se limita su potencia y, por tanto, el alcance real del dispositivo.

3 Cómo resolver los retos de la protección perimetral en aeropuertos

3.1 Nuevas soluciones inteligentes de videovigilancia

La combinación de cámaras de videovigilancia y software de detección de movimiento y basado en la IA ha ampliado el rango y las prestaciones de las soluciones de protección perimetral, desde la simple detección hasta el análisis complejo de los accesos no autorizados.

Un ejemplo son las cámaras térmicas (también conocidas como «termográficas»), que, junto con un software de analítica de vídeo, pueden proteger una zona a cualquier hora del día, independientemente de las condiciones de iluminación. Los sensores que utilizan la tecnología térmica suelen ser muy adecuados para los aeropuertos, puesto que ofrecen la excelente capacidad de detección que requieren las grandes instalaciones.

Los sensores térmicos crean una imagen utilizando la radiación infrarroja emitida por objetos como vehículos o personas, y pueden detectar la actividad a cualquier hora, a distancias significativas y sin que les afecten otros fenómenos que no sean las condiciones meteorológicas más intensas. Cuando se combinan con la analítica de vídeo, las cámaras térmicas modernas con suficiente capacidad de procesamiento son capaces de distinguir entre diferentes tipos de objetos no autorizados y pueden alertar al operador basándose en una lista establecida de condiciones (que incluyen dirección/velocidad/persona/vehículo). Las cámaras tradicionales también pueden hacerlo, pero necesitan la luz visible, que presenta unas limitaciones inherentes y obvias.

Según la legislación local, la tecnología de las cámaras puede utilizarse para supervisar más allá del perímetro físico, proporcionando un margen de vigilancia adicional y brindando al operador un tiempo extra para poder responder. Las soluciones que incorporan la analítica de vídeo permiten activar una alarma según reglas establecidas, por ejemplo, si una persona se acerca a menos de 50 metros de la valla, seguida de un nivel de alarma más alto si esa misma persona se acerca a más de 10 metros, o merodea por encima de un determinado umbral de tiempo en una zona especificada.

En los últimos años, la tecnología de sensores térmicos ha mejorado considerablemente y los costes asociados han disminuido. Los precios competitivos combinados con las soluciones basadas en la tecnología térmica, que proporcionan una supervisión eficaz de largo alcance con cualquier tipo de iluminación y con mal tiempo, son la razón por la que estas soluciones se convierten a menudo en la tecnología de cámara elegida para la detección de intrusos en el perímetro.

4 Costes y servicios prestados

4.1 Evaluación y medición del rendimiento de la inversión

Como ocurre con cualquier medida de seguridad, la evaluación de una solución de protección perimetral debe ser adecuada y proporcionada. Como siempre, la amenaza ha de ser el principal aspecto a tener en

cuenta, que en el caso de un aeropuerto internacional hoy en día puede ser desde manifestantes hasta terroristas, pero al mismo tiempo el sistema debe cumplir con los requisitos normativos pertinentes.

Un enfoque convergente con respecto a la seguridad que incluya aportaciones y consideraciones por parte de otros departamentos, como el de informática y el de operaciones, se está convirtiendo rápidamente en la práctica recomendada. Además, y una cuestión de especial relevancia para los aeropuertos, que cuentan con amplias zonas de acceso restringido, es necesario incluir a las personas implicadas en los requisitos de ingeniería lo antes posible. Históricamente, un buen punto de partida para el perímetro habrían sido las medidas más tradicionales, que suelen disuadir y retrasar a un posible intruso. Solo entonces se pasaría a los sistemas técnicos de detección «complementarios», pero dadas las muchas medidas y sistemas que ahora se integran entre sí, es necesario un enfoque más calculado y holístico desde una fase inicial.

Demostrar la rentabilidad de la inversión de una solución de seguridad es notoriamente difícil. La razón es, principalmente, que no hay ingresos con los que se pueda comparar el coste. Por lo general, el personal de seguridad trabajará con sus compañeros del departamento financiero para determinar el coste de los diferentes tipos de incidentes de seguridad, ya sean costes directos relacionados con la pérdida de activos o daños producidos, o costes más sutiles pero igualmente perjudiciales asociados a la pérdida de reputación de la empresa o de la marca.

Sin embargo, es posible demostrar una ROI (rentabilidad de la inversión) más tangible, sobre todo cuando se utiliza una tecnología que reduce la necesidad de llevar a cabo intervenciones manuales o que permite reasignar al personal a otras tareas. Se pueden encontrar ejemplos en soluciones que no solo alertan al personal de comportamientos sospechosos o accesos no autorizados, sino que también pueden producir respuestas «blandas» automatizadas, como anuncios sonoros o señalización intermitente que informa a los posibles intrusos de que han sido detectados y les insta a abandonar el lugar.

Si hay cámaras que forman parte de la solución, se puede aumentar la eficacia mostrando al intruso que se han grabado algunos datos que le identifican, por ejemplo, utilizando una pantalla para mostrar la matrícula de un vehículo, o incluso una imagen de la propia persona. Solo cuando estas medidas preliminares no producen el efecto deseado es necesario desplegar el equipo de seguridad para emprender una acción más directa. Este planteamiento por fases dirigido a responder a las alertas puede ser más adecuado si se utiliza fuera del perímetro, pero de alguna manera reduce la necesidad de hacer intervenir al personal de seguridad, liberando de este modo recursos, y esto supone un beneficio evidente.

4.2 Evaluación de costes

La estimación de los costes debe basarse en un cálculo del coste total de propiedad (CTP), que incluye todos los costes de la solución a lo largo de su ciclo de vida: los costes materiales y humanos, los costes de los estudios, los costes de instalación del sistema, los costes de funcionamiento, los costes de mantenimiento, los costes de desmantelamiento y de reciclaje. Para ello puede ser necesario adoptar un enfoque diferente por parte de los departamentos de finanzas y compras, ya que podría ser necesario reasignar el capital entre los presupuestos de gastos de explotación y de capital.

5 Soluciones Axis

El enfoque abierto de Axis con respecto a la integración con soluciones de socios significa que nuestras cámaras de red térmicas, combinadas con analítica de vídeo contrastada, permiten a los aeropuertos implementar soluciones de protección perimetral integradas de alto rendimiento que son ciberseguras y rentables durante toda la vida útil del sistema.

En determinadas zonas donde los sensores térmicos podrían no ser tan eficaces, la tecnología de microondas (radar) supone una excelente alternativa, puesto que ofrece muchas de las ventajas de la tecnología

térmica. Las tecnologías de radar y térmica de Axis son capaces de diferenciar entre personas y vehículos, pueden proporcionar información sobre la velocidad y la dirección, pueden integrarse con las cámaras PTZ para realizar un seguimiento eficaz de un objetivo y son adecuadas para cualquier parte de una solución de seguridad en niveles, no solo el perímetro. Los radares de Axis, al igual que las cámaras térmicas, funcionan las 24 horas del día sin interrupción con un número mínimo de falsos positivos, dado que la tecnología no es sensible a los desencadenantes habituales, como las sombras, los cambios de iluminación, los animales pequeños, las gotas de lluvia, los insectos, el viento o el mal tiempo. El ahorro de costes se genera con el tiempo, ya que un menor número de falsos positivos supone menos costes de investigación innecesarios y un equipo de seguridad más pequeño que puede centrarse en las amenazas reales.

A nivel técnico, las cámaras están equipadas con funciones sofisticadas: Estabilización electrónica de imagen (EIS) que gestiona los movimientos de baja y alta amplitud; varios puertos de entrada-salida de alarma para la conexión de hardware externo, y una función de compresión avanzada (Zipstream) para adaptarse a los requisitos de ancho de banda y almacenamiento.

Nuestras cámaras también incorporan los procesadores ARTPEC desarrollados por Axis, con la mejor capacidad del sector, que permiten integrar soluciones de analítica de vídeo para la protección perimetral. Por lo tanto, varias cámaras pueden hacer un seguimiento de varios eventos que tienen lugar de forma simultánea en diferentes lugares. Esta «arquitectura técnica distribuida» permite ampliar la solución a tantas cámaras como sea necesario, y al mismo tiempo prescinde de las inversiones en tecnología de servidores centralizados.

Se detectan cuatro tipos diferentes de eventos, para uno o más individuos o vehículos:

- Acceso no autorizado en una zona predefinida
- • Traspaso de zonas en un orden y una dirección predefinidos
- • Traspaso de zonas condicional
- Detección de personas merodeando

Las cámaras térmicas Axis también funcionan con altavoces IP para emitir mensajes automáticos en caso de detección y advertir a los posibles intrusos.

La tecnología de Axis antes mencionada puede integrarse directamente en el software que se utiliza habitualmente en las plataformas aeroportuarias (Genetec, Milestone, SeeTec, Prysm, etc.).

Para decidir qué equipos se necesitan para habilitar una solución de protección perimetral reforzada y definir el coste de la instalación, se requiere tanto un estudio técnico como una visita sobre el terreno. Axis apoya a los integradores proporcionándoles herramientas de diseño para planificar, diseñar, instalar y gestionar las soluciones.

Las herramientas de diseño de Axis son complementarias y se ofrece asistencia en todas las fases de un proyecto, desde la búsqueda de los productos adecuados en función de criterios específicos hasta la planificación de las instalaciones, y la instalación y gestión de los sistemas. Aprovechar las ventajas que ofrecen las herramientas de Axis ayudará al integrador a poner en marcha los proyectos de una manera más fluida y eficiente.

Las herramientas permiten al integrador elegir los productos adecuados y planificar sistemas optimizados que se basen en estimaciones y sugerencias adaptadas a especificaciones concretas. De este modo, el integrador puede ofrecer la solución adecuada con más rapidez. Las herramientas facilitan incluso la protección de los sistemas que aporta el propio integrador, puesto que el software simplifica la instalación de actualizaciones y parches de seguridad.

6 Referencias de productos

Cámaras térmicas IP: AXIS Q19 Thermal Camera Series

www.axis.com/products/axis-q19-series

Software de análisis: AXIS Perimeter Defender

www.axis.com/products/axis-perimeter-defender

Altavoces IP externos: AXIS C1310-E Network Horn Speaker

www.axis.com/products/axis-c1310-e

Radar IP: Radares de Axis

www.axis.com/products/radars

T10168973/ES/M4.2/2404

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones para mejorar la seguridad y el rendimiento empresarial. Como empresa de tecnología de red y líder del sector, Axis ofrece soluciones de videovigilancia, control de acceso y sistemas de audio e intercomunicación. Se ven reforzadas por aplicaciones de análisis inteligentes y respaldadas por formación de alta calidad.

Axis tiene alrededor de 4000 empleados dedicados en más de 50 países y colabora con socios de integración de sistemas y tecnología en todo el mundo para ofrece soluciones personalizadas. Axis se fundó en 1984 y la sede está en Lund, Suecia