WHITEPAPER

Perimeterschutz für Flughäfen mit intelligenter Videoüberwachung

Überlegungen zur erbrachten Leistung und zur Kapitalrendite

April 2024

AXIS COMMUNICATIONS

Zusammenfassung

Perimeterschutz für Flughäfen umfasst Zäune oder Wände, die die Umgrenzung definieren und ein Eindringen verhindern. Die Umgrenzung sollte außerdem Eindringlinge erkennen und automatisch eine Warnung an die Sicherheitszentrale übermitteln. Die verfügbaren Lösungen für die Erfassung auf dem Gelände und um das Gelände herum können z. B. Kabeldetektoren, Mikrowellensensoren oder Infrarotdrähte sein. Sie sind zwar nützlich, jedoch ist keine davon absolut sicher. Versäumte Erfassungen sind ein Problem, und ein weiteres – ebenso ärgerliches – sind Fehlalarme, die langfristig dazu führen können, dass potenziell ernste Ereignisse völlig ignoriert werden.

Die Kombination von Videoüberwachungskameras mit Bewegungs- und KI-basierter Erkennungssoftware hat das Spektrum und die Möglichkeiten von Perimeterschutzlösungen erweitert, von der einfachen Erkennung bis hin zur komplexen Einbruchsanalyse. Je nach der lokalen Gesetzgebung kann Kameratechnologie zur Überwachung über die physische Eingrenzung hinaus eingesetzt werden, um einen zusätzlichen Überwachungspuffer zu haben und dem Anwender potenziell mehr Reaktionszeit zu lassen.

Die Thermosensortechnologie ist in den letzten Jahren erheblich verbessert worden, und die damit verbundenen Kosten sind gesunken. Wärmebildkameras in Kombination mit Videoanalysesoftware können einen Bereich unabhängig von den Lichtverhältnissen zu jeder Tageszeit schützen. Wärmebildtechnologie ist für Flughäfen oft gut geeignet, da sie ausgezeichnete Erfassungsmöglichkeiten für große Installationen bietet.

Wenn Wärmebildtechnologie nicht eingesetzt werden kann, ist Mikrowellentechnologie (Radar) unter Umständen eine ausgezeichnete Alternative, denn sie bietet viele identische Vorteile. Axis Radar kann zwischen Zielen unterscheiden und lässt sich zur effizienten Verfolgung eines Ziels in PTZ-Kameras integrieren. Diese Technologie funktioniert rund um die Uhr mit minimalen Fehlalarmen und ist aufgrund geringerer Kosten für Untersuchungsverfahren sowie eines kleineren Sicherheitsteams, das sich auf echte Bedrohungen fokussieren kann, mit Einsparungen verbunden.

Die Bewertung einer Lösung zum Perimeterschutz sollte sowohl angemessen als auch verhältnismäßig sein. Höchste Priorität hat immer der Umgang mit Bedrohungen, aber gleichzeitig muss das System alle gesetzlichen Vorschriften einhalten.

Der Nachweis der Kapitalrendite einer Sicherheitslösung ist in der Regel schwierig, da es keine messbaren Einnahmen gibt, die den Kosten gegenübergestellt werden könnten. Allerdings kann die Anwendung von Technologie, die die Notwendigkeit manueller Eingriffe reduziert, konkretere Ergebnisse liefern. Außerdem können Kameras zur Effizienzsteigerung genutzt werden, beispielsweise durch Einsatz eines Bildschirms, der Eindringlingen zeigt, dass Identifizierungsdaten aufgezeichnet wurden.

Kameras von Axis verfügen über anspruchsvolle Funktionen für bessere Bilder, bessere Hardwarekonnektivität und höhere Komprimierung. Außerdem enthalten sie unsere ARTPEC-Prozessoren, mit denen Lösungen für die Videoanalyse zum Perimeterschutz am äußeren Rand des Systems eingebettet werden können. Dank dieser verteilten technischen Architektur wird es möglich, nach Bedarf weitere Kameras hinzuzufügen und dabei Investitionen in eine zentralisierte Serverarchitektur überflüssig werden zu lassen.

Inhalt

1 Einführung

Die Sicherheit eines kritischen Standorts ruht auf zwei Säulen: Design und Schutz. Flughäfen zählen allgemein als Teil der kritischen Infrastruktur eines Landes und müssen Eindringrisiken begrenzen, indem sie geeignete Sicherheitslösungen implementieren, häufig im Rahmen eines strukturierten und mehrschichtigen Konzepts mit physischen Barrieren, Eindringerfassung, Zutrittskontrolle und mobilen Sicherheitspatrouillen.

Die Maßnahmen zum Schutz der kontrollierten Fluggastbereiche eines Flughafens müssen natürlich sowohl die Bedrohungen als auch die Betriebsanforderungen berücksichtigen, insbesondere Überflugrechte, die Topografie des Geländes, spezifische Klimabedingungen und Umweltauflagen. In diesem Whitepaper sollen einige der aktuellen Optionen zum Schutz von Flughäfen erläutert und ein Einblick in die Technologie hinter den Lösungen vermittelt werden.

2 Traditionelle Perimeterschutzlösungen

2.1 Physische Lösungen

Physische Sicherheitslösungen sind oft eine grundlegende Komponente der äußeren Schutzebene eines detaillierten Ansatzes zur Sicherung eines Standorts. In der Regel umfassen sie einen Zaun an der Umgrenzung, der oft aus Draht oder geschweißten Gittern in verschweißten Platten oder Betonplatten besteht. Für die Bereiche in der Nähe von Funknavigations- und Kommunikationsausrüstung werden nicht-magnetische Zäune verwendet. Diese Zäune dienen mehreren Zwecken: Sie sind ein Mittel zur klaren Definition der Flughafengrenzen, schrecken jedoch auch menschliche und tierische Eindringlinge ab. Merkmale wie beispielsweise Kletterschutz, Fahrzeugzufahrten, Passierschutz, Fundamente und Zaunbildschirme können ebenfalls hinzugefügt werden.

Zur Verbesserung der Sicherheit sollte die Umgrenzung mit automatischen Lösungen zur Erfassung von Eindringlingen ausgestattet sein, die bei einem Verstoß einen Alarm zur weiteren Untersuchung an die Sicherheitszentrale senden.

2.2 Eindringerfassung an Zäunen und Toren

Zur Sicherung längerer Umgrenzungen gibt es verschiedene Arten von „Kabelmeldern", die Echtzeitalarme zu einem Sicherheitsmitarbeiter weiterleiten. Einige Lieferanten bieten Zäune, die mit automatischen Erfassungslösungen ausgestattet sind.

Diese Lösungen sind aber nicht hundertprozentig sicher, genausowenig wie Videoüberwachung und alle anderen Lösungen, da sie Fehlalarme (Falschmeldungen) auslösen können. Häufige Ursachen für Fehlalarme sind Tiere, schwankende Bäume und Unwetter. Ohne Videoüberwachung besteht zur Ermittlung des Auslösers nur die Möglichkeit, die Situation von Mitarbeitern untersuchen zu lassen. Wiederholte Fehlalarme können bei den Mitarbeitern Gleichgültigkeit hervorrufen, was unter Umständen dazu führt, dass Warnungen ignoriert werden und eine echte Bedrohung letztlich unbemerkt bleibt.

2.3 Eindringmelder außerhalb von Zäunen

Andere Eindringmelder wie beispielsweise Mikrowellensensoren, Infrarotbarrieren oder Laser werden an strategischen Punkten rund um die Flughafenumgrenzung platziert. Auch hier können Probleme auftreten, wie z. B. Fehlalarme und eingeschränkte Erkennungsmöglichkeiten in Bezug auf Entfernung und Höhe, wenn die Installationsvorschriften nicht strikt eingehalten werden. Der Einsatz von Radar (Mikrowellen)

an der Umgrenzung kann in einer Luftfahrtumgebung aufgrund der Geräte, die vorhandene Technologie im gleichen Spektrum stören, besonders problematisch sein und allein aus diesem Grund ausgeschlossen werden. Die potenziellen Probleme, die mit diesen Geräten verbunden sind, lassen sich durch sorgfältige Auswahl der Frequenz sowie durch Begrenzung ihrer Leistung und damit der effektiven Reichweite des Geräts so gut wie vollständig beseitigen.

3 Herausforderungen für den Perimeterschutz von Flughäfen bewältigen

3.1 Neue, intelligente Videoüberwachungslösungen

Die Kombination von Videoüberwachungskameras mit Bewegungs- und KI-basierter Erkennungssoftware hat das Spektrum und die Möglichkeiten von Perimeterschutzlösungen erweitert, von der einfachen Erkennung bis hin zur komplexen Einbruchsanalyse.

Ein Beispiel hierfür sind Wärmebildkameras (thermografische Kameras), die in Kombination mit Videoanalysesoftware einen Bereich unabhängig von den Lichtverhältnissen zu jeder Tageszeit schützen können. Sensoren, die mit Thermotechnologie arbeiten, sind für Flughäfen oft gut geeignet, denn sie bieten ausgezeichnete Erfassungsmöglichkeiten, die bei großen Installationen erforderlich sind.

Thermosensoren erstellen anhand der von Objekten wie Fahrzeugen oder Personen abgegebenen Infrarotstrahlung ein Bild und können rund um die Uhr mit erheblicher Reichweite Aktivitäten erfassen. Dabei werden sie nur durch schwerste Unwetter beeinträchtigt. In Kombination mit Videoanalyse können moderne Wärmebildkameras mit ausreichender Verarbeitungsleistung zwischen verschiedenen Typen eindringender Objekte unterscheiden und den Sicherheitsmitarbeiter auf der Basis einer festgesetzten Liste von Bedingungen (einschließlich Richtung / Geschwindigkeit / Person / Fahrzeug) warnen. Traditionelle Kameras können das auch, arbeiten dabei jedoch stattdessen mit sichtbarem Licht, was inhärente und offensichtliche Einschränkungen hat.

Je nach der lokalen Gesetzgebung kann Kameratechnologie zur Überwachung über die physische Eingrenzung hinaus eingesetzt werden, um einen zusätzlichen Überwachungspuffer zu haben und dem Anwender potenziell mehr Reaktionszeit zu lassen. Lösungen mit integrierten Videoanalysefunktionen können Alarme nach festen Regeln auslösen, etwa wenn eine Person sich dem Zaun auf weniger als 50 m nähert, gefolgt von einem dringenderen Alarm, wenn sich dieselbe Person auf weniger als 10 m annähert oder sich länger als vorgegeben in einem bestimmten Bereich aufhält.

In den letzten Jahren wurde die Thermosensortechnologie erheblich verbessert, und die damit verbundenen Kosten sind gesunken. Wettbewerbsfähige Preisgestaltung in Kombination mit wärmebasierten Lösungen, die effektive Überwachung großer Reichweite bei jeder Beleuchtung und bei schlechtem Wetter bieten, sind der Grund dafür, dass diese Lösungen oft die bevorzugte Kameratechnologie zur Erfassung von Eindringvorgängen an der Umgrenzung sind.

4 Kosten und erbrachte Leistung

4.1 Bewertung und Messung der Kapitalrendite

Wie bei jeder Sicherheitsmaßnahme sollte die Bewertung einer Lösung zum Perimeterschutz sowohl angemessen als auch verhältnismäßig sein. Wie immer muss die Art der Bedrohung im Vordergrund stehen.

Diese kann bei einem internationalen Flughafen heutzutage von Demonstranten bis hin zu Terroristen reichen, aber gleichzeitig muss das System die relevanten Compliance-Anforderungen einhalten.

Ein abgestimmter Sicherheitsansatz, der auf dem Input und den Überlegungen anderer Abteilungen wie beispielsweise IT und Operations basiert, wird rasch Best Practice. Zusätzlich und besonders relevant für Flughäfen, die große Bereiche mit beschränktem Zugang haben, ist es notwendig, die Personen, die mit den technischen Anforderungen zu tun haben, möglichst früh einzubinden. In der Vergangenheit stellten die traditionelleren Maßnahmen, mit denen typischer Weise ein potenzieller Eindringling abgeschreckt und aufgehalten wurde, einen guten Ausgangspunkt für die Umgrenzung dar. Erst dann ging man zu den ‚strategischen' technischen Erfassungssystemen über, aber bei den vielen Maßnahmen und Systemen, die sich inzwischen integrieren lassen, ist schon vorher ein durchdachteres und ganzheitliches Konzept erforderlich.

Es ist bekanntermaßen schwierig, die Kapitalrendite einer Sicherheitslösung aufzuzeigen. Das ist vor allem darauf zurückzuführen, dass es keine Einnahmen (Erträge) gibt, die den Kosten gegenübergestellt werden könnten. Typischerweise arbeitet das Sicherheitspersonal mit seinen Kollegen in der Finanzabteilung zusammen, um die Kosten verschiedener Arten von Sicherheitsvorfällen zu veranschaulichen; seien es direkte Kosten im Zusammenhang mit dem Verlust / der Beschädigung von Vermögenswerten oder subtilere, aber ebenso schädliche Kosten im Zusammenhang mit dem Verlust des Firmen- oder Markenrufs.

Der Nachweis einer besser konkretisierbaren Kapitalrendite ist allerdings möglich, insbesondere beim Einsatz von Technologie, die die Notwendigkeit manueller Eingriffe reduziert oder zulässt, dass Personal für andere Aufgaben eingeteilt wird. Beispiele finden sich in Lösungen, die nicht nur Mitarbeiter bei verdächtigem Verhalten oder Eindringversuchen warnen, sondern die auch automatisch ‚weiche' Reaktionen produzieren können, etwa hörbare Ankündigungen oder aufleuchtende Hinweise, die potenzielle Eindringlinge darüber informieren, dass sie erfasst wurden, und sie anweisen, den Bereich zu verlassen.

Wenn Kameras Teil der Lösung sind, lässt sich gesteigerte Effizienz erzielen, indem dem Eindringling verdeutlicht wird, dass einige Identifizierungsdaten aufgezeichnet wurden, beispielsweise durch Einsatz eines Bildschirms zur Darstellung eines Fahrzeugkennzeichens oder sogar einer Aufnahme der Person selbst. Erst wenn diese vorbereitenden Maßnahmen nicht die gewünschte Wirkung erzielen, muss das Sicherheitsteam für weitere Aktionen eingesetzt werden. Dieses abgestufte Konzept zur Reaktion auf Warnungen ist möglicherweise besser geeignet für die Anwendung außerhalb des Geländes, aber es kann dazu beitragen, die Notwendigkeit der Einbeziehung von Sicherheitspersonal zu minimieren und so Ressourcen freizusetzen, was einen klaren Vorteil hat.

4.2 Kostenberechnung

Die Kostenschätzung sollte auf einer TCO-Berechnung (Gesamtbetriebskosten) beruhen, bei der alle Kosten der Lösung über ihren gesamten Lebenszyklus einbezogen sind: Material- und Arbeitskosten, Studienkosten, Systeminstallationskosten, Betriebskosten, Wartungskosten, Außerbetriebnahme- und Recyclingkosten. Dazu könnte ein anderes Konzept in den Finanz- und Beschaffungsabteilungen erforderlich sein, denn unter Umständen muss Kapital zwischen den Betriebs- und Investitionskostenbudgets umgeschichtet werden.

5 Lösungen von Axis

Das offene Konzept von Axis für die Integration von Partnerlösungen ermöglicht es Flughäfen, aus einer Kombination von Axis IP-Wärmebildkameras und modernsten Videoanalysefunktionen integrierte Hochleistungs-Perimeterschutzlösungen zu schaffen, die über die gesamte Lebensdauer des Systems cybersicher und kosteneffizient sind.

In bestimmten Bereichen, in denen sich Wärmebildsensoren als weniger effektiv erweisen könnten, ist Mikrowellentechnologie (Radar) eine großartige Alternative, denn sie bietet viele der Vorteile von Wärmebildtechnologie. Die Axis Radar- und Wärmebildtechnologie kann zwischen Personen und Fahrzeugen unterscheiden, Geschwindigkeits- und Richtungsinformationen liefern, zur effektiven Verfolgung eines Ziels in PTZ-Kameras integriert werden und eignet sich für jeden Teil einer mehrschichtigen Sicherheitslösung – nicht nur die Umgrenzung. Axis Radar funktioniert ebenso wie die Wärmebildtechnologie aufgrund seiner Unempfindlichkeit gegenüber üblichen Auslösern wie Schatten, Lichtwechsel, kleinen Tieren, Regentropfen, Insekten, Wind oder Unwetter rund um die Uhr mit minimalen Fehlalarmen. Im Laufe der Zeit ergeben sich Einsparungen, denn weniger Fehlalarme bedeuten weniger unnötige Untersuchungskosten sowie ein kleineres Sicherheitsteam, dass sich auf echte Bedrohungen fokussieren kann.

Auf technischer Ebene verfügen die Kameras über anspruchsvolle Funktionen: Elektronische Bildstabilisierung (Electronic Image Stabilization, kurz EIS) für den Umgang mit kleinen und großen Bewegungsamplituden; mehrere Ein- und Ausgangs-Ports zum Anschluss externer Hardware und eine hochentwickelte Komprimierungsfunktion (Zipstream) zur Anpassung von Bandbreite- und Speicherbedarf.

Axis Kameras verfügen außerdem über unsere ARTPEC-Prozessoren, die branchenweit die höchste Kapazität bieten. Diese ermöglichen eine Integration von Lösungen zur Videoanalyse für den Perimeterschutz. So können mehrere Kameras mehrere Ereignisse verfolgen, die gleichzeitig an verschiedenen Standorten eintreten. Dank dieser so genannten verteilten technischen Architektur kann die Lösung auf so viele Kameras wie erforderlich ausgeweitet werden, während Investitionen in zentralisierte Servertechnologie überflüssig werden.

Vier verschiedene Typen von Ereignissen werden für eine oder mehrere Personen oder Fahrzeuge erfasst:

- Eindringen in einen vordefinierten Bereich
- Überqueren von Zonen in einer vordefinierten Reihenfolge und Richtung
- Bedingtes Überqueren von Zonen
- Unbefugter Aufenthalt

Axis Wärmebildkameras lassen sich auch mit IP-Lautsprechern kombinieren, um bei der Erfassung automatische Meldungen auszugeben, mit denen potenzielle Eindringlinge gewarnt werden.

Die vorerwähnte Axis Technologie lässt sich direkt in Software integrieren, die üblicherweise auf Flughafenplattformen genutzt wird (Genetec, Milestone, SeeTec, Prysm und andere).

Um festzustellen, welche Ausstattung für eine Lösung zum erhöhten Perimeterschutz benötigt wird und um die Installationskosten zu eruieren, sind sowohl eine Schreibtischstudie als auch ein Besuch vor Ort erforderlich. Axis unterstützt Integratoren, indem wir ihnen Designtools für Planung, Design, Installation und Verwaltung der Lösungen bereitstellen.

Die Design-Tools von Axis sind kostenlos und bieten Unterstützung in jeder Phase eines Projekts - von der Auswahl der richtigen Produkte auf der Grundlage spezifischer Kriterien über die Standortplanung bis hin zur Installation und Verwaltung der Systeme. Nutzen Sie die Vorteile von Axis Tools, die dem Integrator bei einer reibungslosen und effizienten Projektdurchführung helfen.

Mithilfe der Tools können die Integratoren basierend auf Abschätzungen und maßgeschneiderten Vorschlägen die passenden Produkte auswählen und optimierte Systeme für die jeweiligen Spezifikationen planen. Anders ausgedrückt: Sie können schneller die passende Lösung liefern. Mit den Tools ist es sogar einfacher, für die ständige Sicherheit der vom Integrator bereitgestellten Systeme zu sorgen, denn mit der Software lassen sich Verbesserungen und Sicherheits-Patches ohne Weiteres installieren.

6 Produktreferenzen

IP-Wärmebildkameras: AXIS Q19 Thermal Camera Serie

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

Analysesoftware: AXIS Perimeter Defender

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

Externe IP-Lautsprecher: AXIS C1310-E Network Horn Speaker

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

IP-Radar: Axis Radargeräte

www.axis.com/de-de/products/radars

T10168973/DE/M4.2/2404

Über Axis Communications

Axis ermöglicht eine intelligente und sichere Welt durch Lösungen zur Verbesserung der Sicherheit und Geschäftsperformance. Als Unternehmen für Netzwerktechnologie und Branchenführer bietet Axis Lösungen in den Bereichen Videosicherheit, Zutrittskontrolle sowie Intercoms und Audiosysteme. Sie werden verstärkt durch intelligente Analyseanwendungen und unterstützt durch gute Schulungen.

Axis beschäftigt rund 4.000 engagierte Mitarbeiter in über 50 Ländern und arbeitet weltweit mit Technologie- und Systemintegrationspartnern zusammen, um den Kunden Lösungen anbieten zu können. Axis wurde 1984 gegründet und der Hauptsitz befindet sich in Lund, Schweden