

Protezione perimetrale per gli aeroporti con videosorveglianza intelligente

Riflessioni sul servizio e sul ritorno sull'investimento

Aprile 2024

Sommario

Tradizionalmente, la protezione perimetrale degli aeroporti è affidata a recinzioni o muri che definiscono il perimetro e prevengono le intrusioni. Il perimetro deve anche essere dotato di un sistema di rilevamento intrusioni che invia allarmi a una centrale di monitoraggio. Alcuni esempi di soluzioni disponibili per il rilevamento perimetrale sono i rilevatori con cavo, i sensori a microonde e le barriere a infrarossi. Pur essendo utili, nessuna di queste è infallibile. I mancati rilevamenti sono il primo problema; il secondo, altrettanto serio, sono i falsi positivi, che a lungo andare possono far sì che episodi potenzialmente gravi vengano totalmente ignorati.

La combinazione tra le telecamere di videosorveglianza e i software per il rilevamento del movimento o basati su IA ha ampliato la gamma e le capacità delle soluzioni di protezione perimetrale, passando dal semplice rilevamento alle analisi complesse delle intrusioni. In base alle leggi locali, è possibile utilizzare le telecamere per monitorare oltre il perimetro fisico; in questo modo si ha una modalità di sorveglianza aggiuntiva e gli operatori hanno più tempo per intervenire.

Le tecnologie a sensori termici sono migliorate notevolmente negli ultimi anni, mentre il loro costo è diminuito. Le telecamere termiche abbinate ai software videoanalitici possono proteggere un'area a qualsiasi ora e in qualsiasi condizione di illuminazione. Spesso, la tecnologia termica è molto adatta per gli aeroporti perché offre ottime funzionalità di rilevamento per grandi installazioni.

Quando non è possibile utilizzare la tecnologia termica, un'alternativa valida può essere la tecnologia a microonde (radar), che offre vantaggi simili. Il radar Axis è in grado di distinguere gli obiettivi e può integrarsi con le telecamere PTZ per seguirli con efficacia. Questa tecnologia funziona 24 ore su 24 e 7 giorni su 7, con pochissimi falsi positivi. In questo modo si risparmia denaro per le indagini, così che un team di sicurezza possa concentrarsi solo sui pericoli concreti.

La valutazione di una soluzione di protezione perimetrale deve essere appropriata e proporzionata. Affrontare le minacce è sempre il primo pensiero ma, al tempo stesso, il sistema deve rispettare tutti i requisiti di legge.

In genere, dimostrare il ritorno sull'investimento di una soluzione di sicurezza è difficile, perché non ci sono ricavi da riportare ai costi. Tuttavia, una tecnologia che riduce la necessità di interventi manuali può offrire risultati più tangibili. Le telecamere possono anche essere utilizzate per aumentare l'efficienza: ad esempio, uno schermo può mostrare agli intrusi che sono stati registrati dati in grado di identificarli.

Le telecamere Axis sono dotate di funzioni sofisticate con immagini di qualità superiore, una migliore connettività dell'hardware e una maggiore compressione. Inoltre, sono dotate del nostro processore ARTPEC, consentendo di integrare le soluzioni analitiche di protezione perimetrale in modalità edge. Questa architettura tecnica distribuita permette di aggiungere altre telecamere secondo le necessità, eliminando gli investimenti sulle tecnologie centralizzate con server.

Sommario

1	Introduzione	4
2	Soluzioni tradizionali di protezione perimetrale	4
	2.1 Soluzioni fisiche	4
	2.2 Rilevamento di intrusioni su recinzioni e cancelli	4
	2.3 Rilevatori di intrusi esterni alle recinzioni	4
3	Le criticità della protezione perimetrale negli aeroporti	5
	3.1 Nuove soluzioni di videosorveglianza intelligenti	5
4	Costi e servizio	5
	4.1 Valutazione e misurazione del ritorno sull'investimento	5
	4.2 Valutazione dei costi	6
5	Soluzioni Axis	6
6	Riferimenti ai prodotti	7

1 Introduzione

La sicurezza di un sito strategico si basa su due pilastri: progettazione e protezione. In genere, gli aeroporti sono considerati parte delle infrastrutture critiche di una nazione e devono limitare i rischi di intrusione con soluzioni di sicurezza adatte, adottando un approccio strutturato e a livelli composto da barriere fisiche, rilevamento intrusioni, controllo accessi e giri di ispezione.

Naturalmente, le misure utilizzate per proteggere le aree vietate di un aeroporto devono tenere in considerazione sia le minacce che i requisiti operativi, in particolare le servitù aeronautiche, la topografia del terreno, le specifiche condizioni climatiche e i vincoli ambientali. Questo documento tecnico descrive alcune soluzioni disponibili per proteggere gli aeroporti e ne approfondisce le rispettive tecnologie.

2 Soluzioni tradizionali di protezione perimetrale

2.1 Soluzioni fisiche

Quando si adotta un approccio a compartimenti per proteggere un sito, spesso le soluzioni fisiche sono una componente fondamentale del "livello esterno". In genere sono costituite da una recinzione perimetrale in rete metallica o elettrosaldata, a pannelli metallici o in cemento armato. Nelle aree vicine ad apparecchiature di radionavigazione e comunicazione si utilizzano reti non magnetiche. Queste recinzioni sono multiuso: definiscono chiaramente i confini dell'aeroporto ma rilevano anche le intrusioni di persone e animali. È anche possibile aggiungere accessori come dispositivi antiscavalco, percorsi per l'accesso di veicoli, dispositivi anti attraversamento, fondamenta e schermature per recinzioni.

Per incrementare la sicurezza, il perimetro deve essere dotato di soluzioni automatiche per il rilevamento delle intrusioni, che possono inviare un allarme a una centrale di monitoraggio per indagare ulteriormente in caso di violazioni.

2.2 Rilevamento di intrusioni su recinzioni e cancelli

Per proteggere lunghi perimetri esistono diversi tipi di "rilevatori" con cavo, che inviano allarmi in tempo reale a un operatore di sicurezza. Alcuni produttori offrono recinzioni dotate di soluzioni di rilevamento automatiche.

Queste soluzioni, così quelle di videosorveglianza o di qualsiasi altro tipo, non sono infallibili e possono generare falsi allarmi, detti "falsi positivi". Le cause più comuni sono gli animali, gli alberi smossi dal vento e gli eventi atmosferici. Senza la videosorveglianza, l'unico modo di verificare la causa dell'allarme è inviare qualcuno per indagare sul posto. Se si ripetono nel tempo, i falsi positivi possono rendere apatico il personale, che può eventualmente ignorare gli allarmi e i pericoli concreti.

2.3 Rilevatori di intrusi esterni alle recinzioni

Altri rilevatori di intrusioni, come i sensori a microonde, le barriere a infrarossi o i laser, vengono posizionati in punti strategici intorno al perimetro dell'aeroporto. Anche queste soluzioni possono essere limitate da problemi quali i falsi positivi e la riduzione della distanza e dell'altezza di rilevamento, se non si seguono rigorosamente le regole di installazione. L'uso dei radar (microonde) sul perimetro può essere particolarmente problematico in ambito aeronautico, perché i dispositivi possono interferire con le tecnologie che operano nello stesso spettro ed essere scartati anche solo per questo. I potenziali problemi

causati da questi dispositivi possono essere eliminati selezionando attentamente la frequenza e limitando la potenza d'esercizio (che però ne riduce anche la portata efficace).

3 Le criticità della protezione perimetrale negli aeroporti

3.1 Nuove soluzioni di videosorveglianza intelligenti

La combinazione tra le telecamere di videosorveglianza e i software per il rilevamento del movimento o basati su IA ha ampliato la gamma e le capacità delle soluzioni di protezione perimetrale, passando dal semplice rilevamento alle analisi complesse delle intrusioni.

Un esempio sono le telecamere termiche (dette anche termografiche) che, se abbinate a un software videoanalitico, possono proteggere un'area a qualsiasi ora e in qualsiasi condizione di illuminazione. Spesso, i sensori a tecnologia termica sono molto adatti agli aeroporti perché offrono ottime funzionalità di rilevamento per grandi sistemi.

I sensori termici creano un'immagine utilizzando le radiazioni a infrarossi emesse da oggetti come veicoli o persone e possono rilevare attività 24 ore su 24, a distanze significative e senza essere condizionati dai fenomeni atmosferici più estremi. Se abbinate alle analitiche video, le moderne telecamere termiche con potenza di calcolo sufficiente sono in grado di distinguere vari tipi di oggetti e intrusi e possono avvisare l'operatore in base a una serie predefinita di condizioni (come direzione/velocità/persona/veicolo). Anche le tradizionali telecamere sono in grado di farlo, ma sfruttano la luce visibile, che ha limitazioni intrinseche ed evidenti.

In base alle leggi locali, è possibile utilizzare le telecamere per monitorare oltre il perimetro fisico; in questo modo si ha una modalità di sorveglianza aggiuntiva e gli operatori hanno più tempo per intervenire. Le soluzioni che impiegano le analitiche video consentono di attivare un allarme in base a regole predefinite, ad esempio quando una persona si avvicina a 50 metri dalla recinzione. Se la persona si avvicina a 10 metri o si aggira con fare sospetto in un'area per un tempo superiore a una soglia preimpostata, si attiva un allarme di livello superiore.

Negli ultimi anni, le tecnologie a sensori termici sono migliorate notevolmente, mentre il loro costo è diminuito. I prezzi concorrenziali, oltre alla capacità di monitorare a lunga distanza, in qualsiasi condizione di illuminazione e con il maltempo, sono i motivi per cui le soluzioni a tecnologia termica sono spesso le preferite per il rilevamento delle intrusioni nel perimetro.

4 Costi e servizio

4.1 Valutazione e misurazione del ritorno sull'investimento

Come per qualsiasi misura di sicurezza, la valutazione di una soluzione di protezione perimetrale deve essere appropriata e proporzionata. Come sempre, il primo pensiero deve essere rivolto alle minacce, che per un aeroporto internazionale possono spaziare dai manifestanti ai terroristi, ma allo stesso tempo il sistema deve rispettare i requisiti di conformità pertinenti.

Un approccio convergente alla sicurezza che include l'input e le considerazioni di altri dipartimenti, come il reparto IT e operativo, sta diventando velocemente la prassi ottimale. Soprattutto per gli aeroporti, che hanno grandi aree ad accesso vietato, è anche necessario coinvolgere al più presto tutte le persone che si

occupano dei requisiti di progettazione. In passato, per il perimetro si partiva dalle misure più tradizionali, che in genere dissuadono e ritardano i potenziali intrusi. Solo in una seconda fase si è passati ai sistemi di rilevamento "fissi". Oggi, però, si integrano molti sistemi e tecnologie, dunque è necessario adottare un approccio più ragionato e olistico fin dall'inizio.

Dimostrare il ritorno sull'investimento di una soluzione di sicurezza è notoriamente difficile, soprattutto perché non ci sono entrate (ricavi) da rapportare ai costi. In genere, il personale di sicurezza lavora con i colleghi del dipartimento finanziario per illustrare il costo dei vari incidenti di sicurezza; possono essere costi diretti, associati alla perdita/danneggiamento di risorse, o costi meno evidenti (ma altrettanto pesanti) legati alla perdita di reputazione dell'azienda o del brand.

Dimostrare un ritorno sull'investimento più tangibile, però, è possibile, soprattutto se si utilizza una tecnologia che riduce gli interventi manuali o consente di riassegnare il personale ad altre mansioni. Alcuni esempi possono essere le soluzioni che non solo segnalano al personale comportamenti sospetti o intrusioni, ma possono anche attuare risposte "soft", come annunci audio o segnali lampeggianti che invitano i potenziali intrusi ad abbandonare l'area.

Integrando le telecamere nella soluzione, è possibile aumentare l'efficienza mostrando all'intruso che sono stati registrati dati in grado di identificarlo: ad esempio, uno schermo può mostrare la sua targa o una sua foto. Solo quando queste misure preliminari non sortiscono l'effetto desiderato si chiameranno in causa gli addetti alla sicurezza per un intervento più diretto. Questo approccio di risposta a fasi potrebbe essere più adatto all'esterno del perimetro, ma riduce al minimo la necessità di coinvolgere il personale di sicurezza e libera risorse: si tratta di un vantaggio evidente.

4.2 Valutazione dei costi

Il calcolo dei costi deve basarsi sul costo totale di proprietà (TCO), che include tutti i costi della soluzione nell'intero ciclo di vita: materiale e manodopera, studi, installazione dei sistemi, costi operativi, manutenzione, smantellamento e riciclaggio. Questo può richiedere un approccio diverso da parte degli uffici finanziari e acquisti, perché potrebbe essere necessario rivedere i budget per le spese operative e le spese in conto capitale.

5 Soluzioni Axis

Grazie all'approccio aperto di Axis verso l'integrazione con soluzioni dei Partner, le nostre telecamere termiche, abbinate alle analitiche video, consentono agli aeroporti di implementare soluzioni di protezione perimetrale integrate e ad alte prestazioni che sono sicure dal punto di vista informatico e riducono i costi per tutto il ciclo di vita del sistema.

Nelle aree in cui i sensori termici potrebbero non essere così efficaci, una valida alternativa è la tecnologia a microonde (radar), che offre vantaggi simili a quelli della tecnologia termica. La tecnologia radar e le tecnologie termiche Axis sono in grado di distinguere persone e veicoli, possono fornire informazioni sulla velocità e la direzione, possono integrarsi con le telecamere PTZ Axis per seguire con efficacia un obiettivo e sono ideali per qualsiasi parte di una soluzione di sicurezza a livelli – non solo il perimetro. I radar e le telecamere termiche Axis funzionano 24 ore su 24 e 7 giorni su 7 con minimi falsi allarmi, perché la loro tecnologia non è sensibile a comuni fenomeni come ombre, variazioni di illuminazione, piccoli animali, pioggia, insetti, vento o intemperie. I risparmi si accumulano nel tempo: meno falsi positivi significa meno costi superflui per le indagini, oltre a un minor numero di vigilanti che possono concentrarsi solo sui pericoli concreti.

A livello tecnico, le telecamere sono dotate di funzioni sofisticate come lo stabilizzatore elettronico dell'immagine (EIS), che contrasta i movimenti ad alta e bassa ampiezza, diverse porte di ingresso-uscita

allarme per collegare l'hardware esistente e una tecnologia di compressione avanzata (Zipstream) per ridurre la larghezza di banda e lo spazio di archiviazione.

Le telecamere Axis sono anche dotate del nostro processore ARTPEC, che offre le migliori capacità nel settore e consente di integrare soluzioni videoanalitiche di protezione perimetrale. Dunque, diverse telecamere possono seguire più eventi che si verificano in simultanea in punti diversi. Questa cosiddetta architettura tecnica distribuita permette di ampliare la soluzione con tutte le telecamere necessarie, eliminando gli investimenti sulle tecnologie centralizzate con server.

Vengono rilevati quattro tipi di eventi, per una o più persone o veicoli:

- Intrusione in un'area predefinita
- Attraversamento di zone in un ordine e una direzione prestabiliti
- Attraversamento condizionale di zone
- Movimenti sospetti

Le telecamere termiche Axis funzionano anche con gli altoparlanti IP per trasmettere messaggi automatici dopo il rilevamento e avvisare i potenziali intrusi.

Queste tecnologie Axis possono essere integrate direttamente nei software più utilizzati negli aeroporti (Genetec, Milestone, SeeTec, Prysm e altri).

Per determinare i dispositivi necessari per una protezione perimetrale avanzata e definire i costi di installazione, occorrono un progetto e un sopralluogo. Axis supporta gli integratori di sistemi fornendo strumenti di progettazione per studiare, progettare, installare e gestire le soluzioni.

Gli strumenti di progettazione Axis sono gratuiti e utili in ogni fase del progetto – dalla ricerca dei prodotti con criteri specifici, alla progettazione dei siti, fino all'installazione e alla gestione dei sistemi. Utilizzando gli strumenti Axis, gli integratori di sistemi possono realizzare i progetti in modo più rapido ed efficiente.

Gli strumenti consentono all'integratore di sistemi di scegliere i prodotti adeguati e progettare sistemi ottimizzati in base a preventivi e suggerimenti adattati a specifiche particolari. Questo significa che l'integratore può fornire la soluzione giusta più velocemente. Questi strumenti consentono anche di proteggere più facilmente il sistema realizzato dall'integratore, perché il software permette di installare gli aggiornamenti e le patch di sicurezza in totale semplicità.

6 Riferimenti ai prodotti

Telecamere termiche IP: serie AXIS Q19 Thermal Camera

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

Software di analisi: AXIS Perimeter Defender

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

Altoparlanti IP esterni: AXIS C1310-E Network Horn Speaker

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

Radar IP: Radar Axis

www.axis.com/products/radars

Informazioni su Axis Communications

Axis consente un mondo più intelligente e più sicuro creando soluzioni per migliorare la sicurezza e le prestazioni aziendali. Come società di tecnologie di rete e leader nel settore, Axis offre soluzioni nella videosorveglianza, controllo degli accessi, interfono e sistemi audio. Queste sono ottimizzate da applicazioni di analisi intelligente e supportate da formazione di alta qualità.

Axis ha circa 4.000 impiegati dedicati in più di 50 paesi e collabora con partner di tecnologia e integrazione di sistema in tutto il mondo per offrire soluzioni di clienti. Fondata nel 1984, Axis è con sede a Lund, in Svezia