LIVRE BLANC

Protection périmétrique pour les aéroports avec vidéosurveillance intelligente

Réflexions sur le service fourni et le retour sur investissement

Avril 2024

AXIS COMMUNICATIONS

Avant-propos

La protection périmétrique traditionnelle des aéroports se compose généralement de clôtures et de murs, qui définissent le périmètre et évitent les intrusions. Le périmètre devrait également être équipé d'outils de détection contre les intrusions qui envoient des alarmes à un poste de contrôle. Les solutions disponibles pour la détection au niveau d'un périmètre et autour de celui-ci peuvent être, par exemple, des détecteurs par câbles, des capteurs à micro-ondes ou des faisceaux infrarouges. Bien qu'utiles, aucune de ces solutions n'est infaillible. Passer à côté d'une détection est un véritable problème mais il existe un autre souci, tout aussi ennuyeux, ce sont les fausses alarmes qui à la longue peuvent conduire à ignorer complètement des incidents potentiellement sérieux.

La combinaison des caméras de vidéosurveillance et d'un logiciel de détection basé sur le mouvement et l'IA a développé la gamme et les fonctionnalités des solutions de protection périmétrique, d'une simple détection à l'analyse d'intrusions complexes. En fonction de la législation locale, la technologie des caméras peut être utilisée pour contrôler au-delà du périmètre physique, ce qui crée une zone tampon de surveillance supplémentaire et offre éventuellement à l'opérateur plus de temps pour réagir.

La technologie des capteurs thermiques s'est considérablement développée ces dernières années et les coûts associés ont diminué. Les caméras thermiques associées à un logiciel d'analyse vidéo peuvent protéger une zone à tout moment de la journée, quelles que soient les conditions d'éclairage. La technologie thermique convient souvent aux aéroports car elle offre d'excellentes fonctionnalités de détection pour les installations importantes.

Lorsque la technologie thermique ne peut être utilisée, la technologie des micro-ondes (radar) peut être une excellente alternative, car elle offre de nombreux avantages similaires. Le radar Axis peut faire la distinction entre les cibles et peut s'intégrer aux caméras PTZ pour le suivi efficace d'une cible. Cette technologie est disponible 24 h sur 24 et 7 j sur 7 et n'émet que très peu de fausses alarmes, ce qui permet de réaliser des économies grâce à la diminution des frais d'investigation et au recours à une plus petite équipe de sécurité qui peut se focaliser sur les véritables menaces.

L'étude d'une solution de protection périmétrique doit être adaptée et proportionnée. La gestion des menaces représente toujours le principal point d'attention, mais en parallèle le système doit se conformer aux exigences juridiques.

Démontrer le retour sur investissement d'une solution de sécurité s'avère généralement difficile car on ne peut comparer aucun revenu par rapport aux coûts engagés. En revanche, utiliser une technologie qui réduit le recours à une intervention manuelle peut offrir des résultats plus tangibles. Les caméras peuvent également être utilisées pour améliorer l'efficacité, par exemple en utilisant un écran pour montrer aux intrus que des données d'identification ont été enregistrées.

Les caméras Axis sont équipées de fonctions complexes pour l'amélioration des images, de la connectivité matérielle et de la compression. Elles sont également équipées de nos propres processeurs ARTPEC, qui permettent d'intégrer des solutions d'analyse vidéo de protection du périmètre à la périphérie. Cette architecture technique répartie permet d'ajouter plus de caméras si nécessaire, tout en éliminant les investissements dans une technologie de serveur centralisé.

Table des matières

1 Introduction

La sécurité d'un site critique repose sur deux piliers, la conception et la protection. Les aéroports sont généralement considérés comme faisant partie des infrastructures critiques d'un pays et ils doivent limiter les risques d'intrusion en mettant en place des solutions de sécurité adaptées, souvent dans le cadre d'une approche structurée en plusieurs niveaux qui comprend des barrières physiques, la détection des intrusions, le contrôle d'accès et des patrouilles de sécurité mobiles.

Les mesures employées pour protéger les zones réglementées d'un aéroport doivent, bien sûr, envisager à la fois les menaces et les besoins de fonctionnement, en particulier les servitudes aéronautiques, la topographie du terrain, les conditions climatiques spécifiques et les contraintes environnementales. Ce livre blanc est destiné à expliquer certaines options actuelles de protection des aéroports. Il donne un aperçu de la technologie derrière les solutions.

2 Solutions traditionnelles de protection périmétrique

2.1 Solutions physiques

Les solutions physiques sont souvent le composant de base de la « couche extérieure » d'une approche compartimentée de sécurisation d'un site, qui comprend généralement une clôture périmétrique, souvent composée d'un treillis métallique ou d'un grillage soudé dans des panneaux soudés ou des panneaux de béton. Pour les zones à proximité des équipements de communication ou de navigation radio, des clôtures non magnétiques sont utilisées. Ces clôtures ont plusieurs objectifs : elles permettent de définir précisément les limites de l'aéroport, mais elles préviennent également les intrusions de personnes ou d'animaux. Des dispositifs tels que l'anti-escalade, l'anti-franchissement, les itinéraires d'accès pour les véhicules, les fondations et les brise-vues peuvent être ajoutés.

Pour améliorer la sécurité, le périmètre peut être équipé de solutions de détection automatique des intrusions, qui envoient une alarme à un poste de contrôle pour que les agents examinent la violation du périmètre.

2.2 Détection des intrusions sur les clôtures et les portes

Il existe différents types de « détecteurs » par câble disponibles pour la sécurisation des très longs périmètres. Ils redirigent des alarmes en temps réel vers un personnel de sécurité. Certains fournisseurs proposent des clôtures équipées de solutions de détection automatique.

Ces solutions, ainsi que la vidéosurveillance ou toute autre solution, ne sont pas infaillibles et peuvent générer des fausses alarmes, qu'on appelle "faux positifs". Les causes fréquentes de faux positifs comprennent les animaux, les arbres qui se balancent et les conditions météorologiques extrêmes. Sans vidéosurveillance, le seul moyen de vérifier ce qui a déclenché l'alarme, c'est d'envoyer un agent pour examiner les lieux. Des fausses alarmes à répétition peuvent provoquer une certaine indifférence de la part du personnel, ce qui pourrait les conduire à ignorer certaines alertes et au final à passer à côté d'une véritable menace.

2.3 Détecteurs d'intrusion à l'extérieur des clôtures

D'autres détecteurs d'intrusion, tels que les capteurs à micro-ondes, les barrières ou les lasers infrarouges sont positionnés à des emplacements stratégiques autour du périmètre de l'aéroport. Mais ces dispositifs peuvent être limités par des problèmes tels que des fausses alarmes et des capacités de détection limitées en termes de distance et de hauteur si les règles d'installation ne sont pas strictement respectées. L'utilisation du radar (micro-ondes) sur le périmètre peut être particulièrement problématique dans un environnement aéronautique, car les dispositifs interfèrent avec la technologie existante sur le même spectre et peuvent être écartés pour cette simple raison. Les problèmes potentiels posés par ces dispositifs peuvent pratiquement être éliminés par le choix minutieux de la fréquence et par la limitation de leur puissance et donc de la portée réelle du dispositif.

3 Gestion des défis de protection périmétrique des aéroports

3.1 Nouvelles solutions de vidéosurveillance intelligentes

La combinaison des caméras de vidéosurveillance et d'un logiciel de détection basé sur le mouvement et l'IA a développé la gamme et les fonctionnalités des solutions de protection périmétrique, d'une simple détection à l'analyse d'intrusions complexes.

On peut citer en exemple les caméras thermiques (qu'on appelle également caméras thermographiques), qui, associées à un logiciel d'analyse vidéo, peuvent protéger une zone à tout moment de la journée, quelles que soient les conditions d'éclairage. Les capteurs qui utilisent la technologie thermique conviennent souvent aux aéroports car ils offrent d'excellentes fonctionnalités de détection pour les installations importantes.

Les capteurs thermiques créent une image qui utilise la radiation infrarouge émise par les objets tels que les véhicules et les personnes. Ils peuvent détecter une activité 24 h sur 24, à des portées importantes, et ils ne sont affectés par aucun élément extérieur à l'exception des conditions météorologiques les plus extrêmes. Lorsqu'elles sont associées à l'analyse vidéo, les caméras thermiques modernes avec une puissance de traitement suffisante peuvent faire la distinction entre différents types d'objets d'intrusion et peuvent alerter l'opérateur en fonction d'une liste définie de conditions (notamment direction/vitesse/personne/véhicule). Les caméras traditionnelles sont également capables de faire cette distinction mais, elles dépendent de la lumière visible, ce qui représente d'évidentes et inhérentes limites.

En fonction de la législation locale, la technologie des caméras peut être utilisée pour contrôler au-delà du périmètre physique, ce qui crée une zone tampon de surveillance supplémentaire et offre éventuellement à l'opérateur plus de temps pour répondre. Les solutions employant les analyses vidéo permettent de déclencher une alarme en fonction de règles définies, par exemple, si une personne approche à moins de 50 mètres de la clôture, suivie d'un niveau d'alarme plus élevé si cette même personne s'approche à moins de 10 mètres ou si elle maraude plus d'un certain temps dans une zone spécifique.

Ces dernières années, la technologie des capteurs thermiques s'est considérablement développée et les coûts associés ont diminué. Des tarifs compétitifs associés à des solutions basées sur la technologie thermique qui permettent une surveillance longue portée efficace quelles que soient les conditions d'éclairage et les conditions météorologiques sont les raisons pour lesquelles ces solutions sont souvent choisies pour la détection des intrusions périmétriques.

4 Coûts et services rendus

4.1 Estimation et mesure du retour sur investissement

Comme pour toute mesure de sécurité, l'étude d'une solution de protection périmétrique doit être adaptée et proportionnée. Comme toujours, la menace doit être au cœur de l'attention. Actuellement, pour un aéroport international, cette menace peut prendre diverses formes, du manifestant au terroriste, mais en parallèle le système doit respecter les conditions de conformité qui s'appliquent.

Une approche combinée de la sécurité qui inclut les données et l'examen attentif des autres services, tels que le service informatique et le service des opérations, représente actuellement la meilleure pratique. De plus, et c'est particulièrement vrai pour les aéroports, qui disposent de grandes zones à accès règlementé, il est nécessaire d'inclure les personnes concernées par les besoins techniques aussi tôt que possible dans la procédure. Traditionnellement, un bon point de départ en ce qui concerne le périmètre aurait été les mesures les plus traditionnelles, qui habituellement dissuadent et retardent un éventuel intrus. Uniquement par la suite, ces mesures auraient intégré les systèmes de détection techniques en option, mais avec de nombreuses mesures et de nombreux systèmes qui s'intègrent dorénavant les uns aux autres, il est nécessaire d'avoir au plus tôt une approche plus réfléchie et plus holistique.

Démontrer le retour sur investissement d'une solution de sécurité s'avère difficile, c'est bien connu. Et ceci principalement en raison du fait qu'on ne peut comparer aucun revenu par rapport aux coûts engagés. Généralement, le personnel de sécurité travaillera avec les employés du service financier pour illustrer les coûts des différents types d'incident de sécurité, qu'il s'agisse de coûts directs liés à la perte ou à l'endommagement de biens ou de coûts plus subtils mais tout aussi dommageables associés à la perte de réputation de l'entreprise ou de la marque.

Démontrer un retour sur investissement plus tangible est cependant possible, en particulier en utilisant une technologie qui diminue le recours aux interventions manuelles ou qui permet au personnel d'être redéployé sur d'autres tâches. Des exemples peuvent être trouvés dans les solutions qui non seulement alertent le personnel des comportements suspects ou des intrusions, mais qui peuvent également produire des réponses « douces » automatisées, telles que des annonces sonores ou des panneaux lumineux informant les potentiels intrus qu'ils ont été détectés et leur donnant l'ordre de quitter la zone.

Si les caméras font partie de la solution, on peut ensuite augmenter l'efficacité en montrant aux intrus que des données d'identification ont été enregistrées, par exemple en utilisant un écran pour afficher une plaque d'immatriculation d'un véhicule, ou même une image de la personne. Ce n'est que lorsque ces mesures préliminaires n'ont produit aucun effet que l'équipe de sécurité doit être envoyée sur place pour une action plus directe. Cette approche par étape pour répondre aux alertes pourrait être plus adaptée à une utilisation en dehors du périmètre, mais elle permet malgré tout de diminuer dans une certaine mesure le recours au personnel de sécurité, libérant ainsi certaines ressources, ce qui représente un avantage non négligeable.

4.2 Estimation des coûts

L'estimation des coûts sera basée sur le calcul du coût total de possession (CTP), qui comprend tous les coûts de la solution tout au long de son cycle de vie : les coûts matériels et humains, les coûts d'études, les coûts d'installation du système, les coûts de fonctionnement, les frais d'entretien, les frais de mise hors service et de recyclage. Cela peut nécessiter une approche différente de la part des services financiers et des achats, car il faudra peut être réaffecter le capital entre les budgets de dépense d'établissement et de charges d'exploitation.

5 Solutions Axis

L'approche ouverte d'Axis en matière d'intégration de solutions de partenaires signifie que nos caméras thermiques sur IP, associées aux analyses vidéo éprouvées, permettent aux aéroports de mettre en place des solutions de protection périmétrique intégrées de hautes performances, sûres sur le plan de la cybersécurité et rentables tout au long de la durée de service du système.

Dans certains cas, lorsque les capteurs thermiques ne s'avèrent pas si efficaces, la technologie des micro-ondes (radar) représente une formidable alternative, car elle offre de nombreux avantages similaires à la technologie thermique. Les technologie radar et thermiques d'Axis sont capables de distinguer les personnes et les véhicules, elle peut fournir des informations relatives à leur vitesse et leur direction, peut s'intégrer aux caméras PTZ pour un suivi performant d'une cible et convient sur tous les plans d'une solution de sécurité à plusieurs niveaux, pas uniquement pour le périmètre. Les radars Axis, tout comme les caméras thermiques, fonctionnent 24 h sur 24 et 7 j sur 7 et n'émettent que très peu de fausses alarmes, car la technologie n'est pas sensible aux déclencheurs habituels tels que les ombres, les changements de luminosité, les petits animaux, les gouttes de pluie, les insectes, le vent et les mauvaises conditions météorologiques. La réduction des coûts s'accroît avec le temps puisque grâce à la diminution des fausses alarmes, les frais d'investigations inutiles diminuent également et une plus petite équipe de sécurité peut se focaliser sur les véritables menaces.

Au niveau technique, les caméras sont équipées de fonctions complexes : La stabilisation d'image électronique (EIS) qui gère les mouvements de grande et de faible amplitude ; plusieurs ports entrée-sortie d'alarme pour brancher du matériel externe ; et une fonction avancée de compression (Zipstream) pour répondre aux besoins de stockage et de bande passante.

Les caméras Axis sont également équipées de nos propres processeurs ARTPEC, offrant la meilleure capacité du secteur, ce qui permet l'intégration de solutions d'analyse vidéo pour la protection périmétrique. Plusieurs caméras peuvent par conséquent suivre plusieurs événements qui se produisent en même temps à différents endroits. Cette architecture que l'on nomme architecture technique distribuée permet d'étendre la solution à autant de caméras que nécessaire, tout en éliminant les investissements dans une technologie de serveur centralisé.

Quatre types d'événement différents sont détectés, pour un ou plusieurs individus ou véhicules :

- • Intrusion dans une zone prédéfinie
- • Franchissement de zones dans un ordre et un sens déterminés
- • Franchissement de zone conditionnel
- • Maraudage

Les caméras thermiques sur IP fonctionnent également avec des haut-parleurs sur IP qui émettent des messages automatiques à destination des potentiels intrus lorsque ceux-ci sont détectés.

La technologie Axis mentionnée ci-dessus peut être intégrée directement dans les logiciels fréquemment utilisés dans les plateformes d'aéroports (Genetec, Milestone, SeeTec, Prysm, et d'autres).

Pour établir l'équipement requis pour renforcer une solution de protection périmétrique et définir les coûts d'installation, une étude documentaire et une visite sur site sont nécessaires. Axis soutient les intégrateurs en fournissant des outils de conception pour planifier, concevoir, installer et gérer les solutions.

Les outils de conception Axis sont offerts à titre gracieux et une assistance est fournie à toutes les étapes du projet, de la sélection des bons produits en fonction de critères spécifiques à l'organisation des sites et à l'installation et la gestion des systèmes. Les outils Axis permettront à l'intégrateur de réaliser les projets plus facilement et plus efficacement.

Les outils permet à l'intégrateur de sélectionner les produits adaptés et de dessiner des systèmes optimisés basés sur des estimations et des suggestions adaptées à des caractéristiques techniques particulières. Cela signifie que l'intégrateur peut fournir plus rapidement la meilleure solution. Les outils permettent même de rendre les systèmes fournis par l'intégrateur plus sûrs, car le logiciel simplifie l'installation de mises à niveau et de correctifs de sécurité.

6 Références des produits

Caméras thermiques sur IP : série de caméra thermique AXIS Q19

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

Logiciel d'analyse : AXIS Perimeter Defender

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

Haut-parleurs externes sur IP : AXIS C1310-E Network Horn Speaker

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

Radar sur IP: Radars Axis

www.axis.com/products/radars

À propos d'Axis Communications

En concevant des solutions qui améliorent la sécurité et les performances de l'entreprise, Axis crée monde plus clairvoyant et plus sûr. En tant qu'entreprise de technologie de réseau et leader de l'industrie, Axis propose des solutions de vidéosurveillance, de contrôle d'accès, d'interphonie et de systèmes audio. Les performances de ces solutions sont améliorées grâce à des applications d'analyse intelligentes et une formation de haute qualité.

Axis emploie près de 4 000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et d'intégration de systèmes dans le monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984 et le siège social se trouve à Lund, en Suède