WHITE PAPER

Proteção de perímetro para aeroportos com videomonitoramento inteligente

Reflexões sobre o serviço prestado e o retorno do investimento

Julho 2021

AXIS COMMUNICATIONS

Sumário

1 Resumo

A proteção de perímetro tradicional para aeroportos normalmente consiste em cercas ou muros, que definem o perímetro e evitam intrusões. O perímetro deve também ser equipado com detecção de intrusão que envia alarmes para uma estação de monitoramento. As soluções disponíveis para detecção dentro e ao redor do perímetro podem ser, por exemplo, detectores de cabo, sensores de micro-ondas ou sensores de barreira infravermelhos. Embora úteis, nenhum deles é infalível. As detecções perdidas são um problema e outro, igualmente preocupante, são os falsos positivos, que, a longo prazo, podem fazer com que incidentes potencialmente graves sejam completamente ignorados.

A combinação de câmeras de videomonitoramento e software de detecção de movimento expandiu a faixa e as capacidades das soluções de proteção de perímetro, de simples detecção a análises de intrusão complexas. Dependendo da legislação local, a tecnologia de câmera pode ser usada para monitorar além do perímetro físico, fornecendo um buffer de monitoramento adicional e potencialmente permitindo ao operador tempo extra para responder.

A tecnologia de sensor térmico foi significativamente aprimorada nos últimos dias e os custos associados a ela diminuíram. As câmeras térmicas acopladas a um software de análise de vídeo podem proteger uma área a qualquer hora do dia, independentemente das condições de iluminação. A tecnologia térmica costuma ser adequada para aeroportos, pois oferece excelentes recursos de detecção para grandes instalações.

Onde a terminologia térmica não pode ser usada, a tecnologia de micro-ondas (radar) pode ser uma excelente alternativa, já que oferece muitos dos mesmos benefícios. O radar Axis pode diferenciar alvos e pode se integrar a câmeras PTZ para rastreamento eficaz de um alvo. Esta tecnologia funciona 24 horas por dia, 7 dias por semanas, com o mínimo de falsos positivos, proporcionando economia devido a menos custos de investigação, bem como uma equipe de segurança menor que pode se concentrar em ameaças reais.

A avaliação de uma solução de proteção de perímetro deve ser apropriada e proporcional. Lidar com as ameaças é sempre a consideração principal, mas, ao mesmo tempo, o sistema deve cumprir com todos os requisitos legais.

Demonstrar o retorno sobre o investimento para uma solução de segurança é geralmente difícil, já que não há receita para medir em relação ao custo. No entanto, o uso da tecnologia reduz a necessidade para intervenção manual pode fornecer resultados mais tangíveis. As câmeras também podem ser usadas para aumentar a eficiência, por exemplo, usando uma tela para mostrar os invasores cujos dados de identificação foram registrados.

As câmeras Axis são equipadas com funções sofisticadas para obter imagens aprimoradas, melhor conectividade de hardware e maior compactação. Elas também possuem seus próprios processadores ARTPEC da Axis, que permitem que soluções de análise de vídeo para proteção de perímetro sejam incluídas na borda. Esta arquitetura técnica distribuída torna possível a adição de mais câmeras conforme necessário, enquanto elimina investimentos em tecnologia de servidor centralizado.

2 Introdução

A segurança de um site crítico se baseia em dois pilares: desenho e proteção. Os aeroportos são comumente considerados parte da infraestrutura crítica de uma nação e são obrigados a limitar os riscos de intrusão, implementando soluções de segurança adequadas, muitas vezes como parte de uma abordagem estruturada e em camadas que incorpora barreiras físicas, detecção de intrusão, controle de acesso e patrulhas de segurança móvel.

As medidas usadas para proteger áreas restritas de um aeroporto devem, é claro, considerar a ameaça e os requisitos operacionais, em particular **servidões** aeronáuticas, a topografia do terreno, condições climáticas

específicas e restrições ambientais. Este white paper tem por objetivo explicar algumas das opções atuais para proteger aeroportos e fornecer uma visão sobre a tecnologia por trás das soluções.

3 Soluções de proteção de perímetro tradicional

3.1 Soluções físicas

As soluções físicas normalmente são um componente fundamental da "camada externa" de uma abordagem compartimentalizada para proteger um site, normalmente compreendendo uma cerca de perímetro, muitas vezes construída de arame ou malha soldada, em painéis soldados ou painéis concretos. Para as áreas próximas a equipamentos de navegação e comunicações por rádio, utilizam-se cercas não magnéticas. Essas cercas são multiuso: são um meio de claramente definir os limites de um aeroporto, mas elas também impedem intrusões de pessoas e animais. Recursos como dispositivos antiescalada, rotas de acesso de veículo, dispositivos anticruzamento, fundações e telas de cerca também podem ser adicionados.

Para melhorar a segurança, o perímetro deve ser equipado com soluções de detecção de intrusão automática, que envia um alarme para uma estação de monitoramento para investigação adicional, caso ocorra uma violação.

3.2 Detecção de intrusão em cercas e portões

Há tipos diferentes de "detectores" de cabo disponíveis para proteger perímetros extensos e redirecionam alarmes em tempo real para um operador de segurança. Alguns fornecedores oferecem cercas equipadas com soluções de detecção automática.

Estas soluções, no entanto, não são infalíveis e podem gerar alarmes falsos, chamados de "falsos positivos". As causas comuns de falsos positivos incluem animais, plantas e árvores em movimento e clima severo. Sem videomonitoramento, a única maneira de verificar o que causou o alarme é enviar uma equipe para investigar. Falsos positivos repetidos podem levar à apatia entre a equipe, possivelmente resultando em alertas sendo ignorados e uma ameaça real, em última análise, sendo perdida.

3.3 Detectores de intrusão fora das cercas

Outros detectores de intrusão, tais como sensores de micro-ondas, barreiras infravermelhas ou lasers, são posicionados em locais estratégicos ao redor do perímetro do aeroporto. Novamente, isso pode ser restringido por questões como falsos positivos e recursos de detecção limitados para distância e altura se as regras de instalação não forem estritamente seguidas. O uso de radar (micro-ondas) no perímetro pode ser particularmente problemático em um ambiente de aviação, devido aos dispositivos interferindo com a tecnologia existente no mesmo espectro, e pode ser excluído apenas por essa razão. Os problemas potenciais apresentados por estes dispositivos podem ser praticamente eliminados pela escolha cuidadosa da frequência e pela limitação de sua potência e, portanto, do alcance eficaz do dispositivo.

4 Lidando com os desafios de proteção do perímetro do aeroporto

4.1 Novas soluções de videomonitoramento inteligentes

A combinação de câmeras de videomonitoramento e software de detecção de movimento expandiu a faixa e as capacidades das soluções de proteção de perímetro, de simples detecção a análises de intrusão complexas.

Um exemplo são as câmeras térmicas (também chamadas de termográficas), que, quando acopladas a um software de análise de vídeo, podem proteger uma área a qualquer hora do dia, independentemente das condições de iluminação. Sensores que usam a tecnologia térmica costumam ser adequados para aeroportos, pois eles oferecem excelentes recursos de detecção necessários para grandes instalações.

Os sensores térmicos criam uma imagem usando radiação infravermelha emitida por objetos, tais como veículos ou pessoas, e podem detectar atividades 24 horas por dia, em intervalos significativos, e não são afetados por nada além das condições climáticas mais severas. Quando combinadas com análise de vídeo, as câmeras térmicas modernas com poder de processamento suficiente são capazes de distinguir entre tipos diferentes de objetos de intrusão e podem alertar o operador com base em uma lista definida de condições (incluindo direção/velocidade/pessoa/veículo). As câmeras tradicionais também são capazes de fazer isso, mas contam com luz visível, que possui limitações inerentes e óbvias.

Dependendo da legislação local, a tecnologia de câmera pode ser usada para monitorar além do perímetro físico, fornecendo um buffer de monitoramento adicional e potencialmente permitindo ao operador tempo extra para responder. Soluções que empregam análises de vídeo tornam possível disparar um alarme de acordo com regras definidas, por exemplo, se uma pessoa se aproximar a 50 metros da cerca, seguido por um nível de alarme mais alto no caso dessa mesma pessoa se aproximar a menos de 10 metros, ou está perambulando acima de um certo limite de tempo em uma zona especificada.

Nos últimos dias, a tecnologia de sensor térmico melhorou significativamente e os custos associados diminuíram. O preço competitivo combinado com soluções baseadas em tecnologia térmica, fornecendo monitoramento eficaz de longo alcance em qualquer iluminação e em condições climáticas adversas, é o motivo pelo qual essas soluções são frequentemente a tecnologia de câmera escolhida para detecção de intrusão de perímetro.

5 Custos e serviços prestados

5.1 Avaliação e medição do retorno do investimento

Como com qualquer medida de segurança, a avaliação de uma solução de proteção de perímetro deve ser apropriada e proporcional. Como sempre, a ameaça precisa ser a consideração principal, que para um aeroporto internacional hoje pode ir de manifestantes a terroristas, mas, ao mesmo tempo, o sistema deve aderir a requisitos de conformidade relevantes.

Uma abordagem convergente de segurança que inclui entrada e considerações de outros departamentos, tais como TI e operações, está se tornando prática recomendada rapidamente. Adicionalmente, e de relevância particular para aeroportos, que tem grandes áreas com acesso restrito, há uma necessidade de incluir essas pessoas envolvidas com requisitos de engenharia o mais cedo possível. Historicamente, um bom ponto de partida para o perímetro teria sido as medidas mais tradicionais, que normalmente detêm e atrasam um invasor em potencial. Só então elas passariam para sistemas de detecção técnica extras,

mas com muitas medidas e sistemas agora se integrando entre si, uma abordagem mais considerada e holística é necessária anteriormente.

Demonstrar um retorno do investimento para uma solução de segurança é notoriamente difícil. Isso é principalmente devido ao fato de que não há receita para medir em relação ao custo. Normalmente, o pessoal de segurança trabalhará com seus colegas no departamento de finanças para ilustrar o custo de diferentes tipos de incidente de segurança, sejam eles custos diretos para perda/dano de ativos ou custos mais sutis, mas igualmente prejudiciais, associados com a perda da reputação da empresa ou da marca.

No entanto, demonstrar um ROI mais tangível é possível, particularmente ao usar tecnologia que reduz a necessidade de intervenções manuais ou que permite que a equipe seja realocada para outras tarefas. Os exemplos podem ser encontrados em soluções que não só alertam a equipe quanto a comportamento suspeito ou invasões, mas que podem também produzir respostas "suaves", tais como anúncios audíveis ou sinalização piscando, informando sobre potenciais invasores que foram detectados e os instruindo a deixar a área.

Se as câmeras fizerem parte da solução, então uma maior eficiência pode ser alcançada mostrando ao invasor que alguns dados de identificação foram registrados, por exemplo, usando uma tela para mostrar uma placa de licenciamento de um veículo ou mesmo uma imagem da própria pessoa. Apenas quando estas medidas preliminares não produzem o efeito desejado, a equipe de segurança precisa ser direcionada para uma ação mais direta. Esta abordagem em fases para responder a alertas pode ser mais adequada para uso fora do perímetro, mas de alguma forma minimiza a necessidade de envolver o pessoal de segurança, liberando recursos, o que tem um benefício claro.

5.2 Avaliação do custo

A estimativa de custo deve se basear no cálculo do custo total de propriedade (TCO), que inclui todos os custos da solução por todo o ciclo de vida: os custos materiais e humanos, os custos dos estudos, os custos de instalação do sistema, os custos operacionais, os custos de manutenção, os custos de desativação e de reciclagem. Isso pode exigir uma abordagem diferente dos departamentos de finança e compras, pois pode haver a necessidade de realocar capital entre os orçamentos operacionais e de despesas de capital.

6 Proposta da Axis Communications

A abordagem aberta da Axis para integração com soluções de parceiros significa que suas câmeras de rede térmicas, combinadas com análises de vídeo comprovadas, permitem que os aeroportos implementem soluções de proteção de perímetro integradas de alto desempenho que são ciberseguras e econômicas durante toda a vida útil do sistema.

Em certas áreas, onde os sensores térmicos podem não ser tão eficazes, a tecnologia de micro-ondas (radar) é uma ótima alternativa, pois oferece muitos dos mesmos benefícios que a tecnologia térmica. A tecnologia de radar Axis é capaz de diferenciar entre humanos e veículos, pode fornecer informações de velocidade e direção, pode se integrar com câmeras PTZ para um rastreamento eficaz de um alvo e é adequada para qualquer parte de uma solução de segurança em camadas, não apenas o perímetro. Quanto à térmica, a tecnologia de radar funciona 24 horas por dia, 7 dias por semanas com o mínimo de falsos positivos, pois não é sensível a acionadores comuns, como sombras, mudanças na iluminação, pequenos animais, gotas de chuva, insetos, ventou ou mau tempo. A economia de custos aumenta ao longo do tempo, pois menos falsos positivos significam menos custos desnecessários com investigação, bem como uma equipe menor de segurança que pode se concentrar em ameaças reais.

Em um nível técnico, as câmeras são equipadas com funções sofisticadas: Estabilização Eletrônica de Imagem (EIS), que gerencia movimentos de alta e baixa amplitude, múltiplas portas de entrada-saída de

alarme para conectar hardware externo e uma função de compactação avançada (Zipstream) para atender os requisitos de largura de banda e armazenamento.

As câmeras Axis também possuem seus próprios processadores ARTPEC da Axis, com a melhor capacidade do setor, permitindo que as soluções de análise de vídeo para proteção de perímetro sejam incorporadas. Muitas câmeras podem, portanto, rastrear vários eventos que acontecem simultaneamente em diferentes locais. A chamada arquitetura técnica distribuída permite estender a solução para quantas câmeras forem necessárias, ao mesmo tempo que elimina investimentos em tecnologia de servidor centralizado.

Quatro tipos diferentes de eventos são detectados, para um ou mais indivíduos ou veículos:

- Invasão em uma área predefinida
- Zonas de passagem em ordem e direção predeterminadas
- Passagem de zona condicional
- Perambulação

As câmeras térmicas Axis também funcionam com alto-falantes IP para emitir mensagens automáticas mediante detecção, para alertar possíveis intrusos.

A tecnologia Axis mencionada acima pode ser integrada diretamente a softwares comumente usados em plataformas de aeroporto (Genetec, Milestone, SeeTec, Prysm e outras mais).

Para estabelecer qual equipamento é necessário para ativar uma solução de proteção de perímetro reforçada e definir o custo de instalação. Isso requer um estudo teórico e uma visita ao local. A Axis dá suporte a integradores, fornecendo ferramentas de desenho para planejar, desenhar, instalar e gerenciar as soluções.

As ferramentas de desenho da Axis são gratuitas e é oferecido suporte em cada estágio de um projeto - desde encontrar os produtos certos com base em critérios específicos até o planejamento de sites e instalação e gerenciamento de sistemas. Aproveitar as ferramentas Axis ajudará o integrador a realizar projetos de forma mais suave e eficiente.

As ferramentas permitem que o integrador escolha os produtos apropriados e planeje sistemas otimizados com base em estimativas e sugestões feitas sob medida para especificações específicas, significando que eles podem entregar a solução certa mais rapidamente. As ferramentas facilitam ainda mais manter seguros os sistemas que o integrador fornece, porque o software facilita a instalação de atualizações e patches de segurança.

7 Referências de produto

Câmeras IP térmicas: AXIS Q19 Series

https://www.axis.com/pt-br/products/axis-q19-series

Software de análise: AXIS Perimeter Defender

https://www.axis.com/pt-br/products/axis-perimeter-defender

Alto-falantes IP externos: AXIS C3003-E Network Horn Speaker

https://www.axis.com/pt-br/products/axis-c3003-e

Radar IP

https://www.axis.com/pt-br/products/axis-d2050-ve

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e mais seguro criando soluções de rede que fornecem percepções que permitem melhorar a segurança e encontrar novas formas de fazer negócios. Como líder do setor de vídeo em rede, a Axis oferece produtos e serviços para sistemas de vigilância e análise de vídeo, controle de acesso, intercomunicação e áudio. A Axis conta com mais de 3.800 funcionários dedicados em mais de 50 países e colabora com parceiros em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e sua sede está localizada em Lund, na Suécia.

Para obter mais informações sobre a Axis, visite nosso site *axis.com*.