WHITE PAPER

Perimeter protection for airports with intelligent video surveillance

Reflections on the service rendered and the return on investment

April 2024

AXIS COMMUNICATIONS

Summary

Traditional perimeter protection for airports typically consists of fences or walls, which define the perimeter and prevent intrusion. The perimeter should also be equipped with intrusion detection that sends alarms to a monitoring station. The solutions available for detection on and around the perimeter can be, for example, cable detectors, microwave sensors, or infrared tripwires. Although useful, none of these are foolproof. Missed detections are one problem, and another, equally troublesome, is false positives, which in the long run can lead to potentially serious incidents being ignored completely.

The combination of video surveillance cameras and motion- and AI-based detection software has expanded the range and capabilities of perimeter protection solutions, from simple detection to complex intrusion analysis. Depending on local legislation, camera technology can be used to monitor beyond the physical perimeter, providing an additional surveillance buffer and potentially allowing the operator extra time to respond.

Thermal sensor technology has improved significantly in recent years, and the associated costs have decreased. Thermal cameras coupled with video analytics software can protect an area at any time of day, irrespective of the lighting conditions. Thermal technology is often well suited to airports as it offers excellent detection capabilities for large installations.

Where thermal technology cannot be used, microwave technology (radar) can be an excellent alternative, as it offers many of the same benefits. Axis radar can differentiate between targets and can integrate with PTZ cameras for effective tracking of a target. This technology performs 24/7 with minimal false positives, providing savings due to fewer investigative costs, as well as a smaller security team that can focus on real threats.

Evaluation of a perimeter protection solution should be both appropriate and proportionate. Addressing threats is always the primary consideration, but at the same time the system must comply with all legal requirements.

Demonstrating a Return on Investment for a security solution is generally difficult, as there is no revenue to measure against the cost. However, using technology that reduces the need for manual intervention can provide more tangible results. Cameras can also be used to increase efficiency, for example by using a screen to show intruders that identification data has been recorded.

Axis cameras are equipped with sophisticated functions for improved images, better hardware connectivity, and greater compression. They also feature our own ARTPEC processors, which allow perimeter protection video analytic solutions to be embedded on the edge. This distributed technical architecture makes it possible to add more cameras as necessary, while eliminating investments in centralized server technology.

Table of Contents

1 Introduction

The security of a critical site rests on two pillars: design and protection. Airports are commonly considered part of a nation's critical infrastructure and are required to limit intrusion risks by implementing suitable security solutions, often as part of a structured and layered approach incorporating physical barriers, intrusion detection, access control, and mobile security patrols.

The measures used to protect an airport's restricted areas must, of course, consider both the threat and the operating requirements, in particular aviation easements, the topography of the terrain, specific climatic conditions, and environmental constraints. This white paper aims to explain some of the current options for protecting airports and gives an insight into the technology behind the solutions.

2 Traditional perimeter protection solutions

2.1 Physical solutions

Physical solutions are often a fundamental component of the 'outer layer' of a compartmentalized approach to securing a site, typically comprising a perimeter fence, often constructed of wire or welded mesh, in welded panels or concrete panels. For the areas near radio navigation and communications equipment, non-magnetic fences are used. These fences are multi-purpose: they are a means to clearly define the airport's boundaries, but they also deter intrusions by people and animals. Features such as anti-climbing devices, vehicle access routes, anti-crossing devices, foundations, and fence screens can also be added.

To enhance security, the perimeter should be equipped with automatic intrusion detection solutions, which send an alarm to a monitoring station for further investigation should a breach occur.

2.2 Intrusion detection on fences and gates

There are different types of cable "detectors" available for securing lengthy perimeters, and these redirect real-time alarms to a security operator. Some suppliers offer fences equipped with automatic detection solutions.

These solutions, as well as video surveillance or any other solution, are not foolproof and can generate false alarms, referred to as "false positives". Common causes of false positives include animals, swaying trees, and severe weather. Without video surveillance, the only way to verify what caused the alarm is to dispatch personnel to investigate. Repeated false positives may lead to apathy amongst staff, possibly resulting in alerts being ignored and a real threat ultimately being missed.

2.3 Intrusion detectors outside fences

Other intrusion detectors, such as microwave sensors, infrared barriers or lasers are positioned at strategic locations around the perimeter of the airport. Again, these can be constrained by issues such as false positives and limited detection capabilities for distance and height if the installation rules are not followed strictly. The use of radar (microwaves) on the perimeter can be particularly problematic in an aviation environment, due to the devices interfering with existing technology on the same spectrum and can be precluded for this reason alone. The potential problems posed by these devices can be all but eliminated by the careful choice of frequency and by limiting their power and thus the effective range of the device.

3 Addressing airport perimeter protection challenges

3.1 New intelligent video surveillance solutions

The combination of video surveillance cameras and motion- and AI-based detection software has expanded the range and capabilities of perimeter protection solutions, from simple detection to complex intrusion analysis.

One example is thermal (also referred to as thermographic) cameras, which, when coupled with video analytics software, can protect an area at any time of day, irrespective of the lighting conditions. Sensors using thermal technology are often well suited to airports as they offer excellent detection capabilities required for large installations.

Thermal sensors create an image using infrared radiation emitted by objects such as vehicles or persons, and can detect activity around the clock, at significant ranges, and unaffected by anything but the most severe weather conditions. When combined with video analytics, modern thermal cameras with sufficient processing power are able to distinguish between different types of intrusion objects and can alert the operator based on a set list of conditions (including direction/speed/person/vehicle). Traditional cameras are also able to do this, but rely instead on visible light, which has inherent and obvious limitations.

Depending on the local legislation, camera technology can be used to monitor beyond the physical perimeter, providing an additional surveillance buffer and potentially allowing the operator extra time to respond. Solutions employing video analytics make it possible to trigger an alarm according to set rules, for example, if a person approaches within 50 meters of the fence, followed by a higher alarm level if that same person comes closer than 10 meters, or is loitering above a certain time threshold in a specified zone.

In recent years, thermal sensor technology has improved significantly, and the associated costs have decreased. Competitive pricing combined with thermal based solutions providing effective long-range monitoring in any lighting and in bad weather is why these solutions are often the chosen camera technology for perimeter intrusion detection.

4 Costs and service rendered

4.1 Evaluation and measuring the return on investment

As with any security measure, evaluation of a perimeter protection solution should be both appropriate and proportionate. As always, the threat needs to be the primary consideration, which for an international airport today can range from protestors to terrorists, but at the same time the system must adhere to relevant compliance requirements.

A converged approach to security that includes input and considerations from other departments, such as IT and operations, is fast becoming best practice. Additionally, and of particular relevance to airports, which have large areas with restricted access, there is a need to include those persons involved with the engineering requirements as early as possible. Historically, a good starting point for the perimeter would have been the more traditional measures, which typically deter and delay a potential intruder. Only then would they move on to the 'bolt on' technical detection systems, but with many measures and systems now integrating with each other, a more considered and holistic approach is required earlier on.

Demonstrating a Return on Investment for a security solution is notoriously difficult. This is mainly due to the fact that there is no income (revenue) to measure against the cost. Typically, security personnel will

work with their colleagues in the finance department to illustrate the cost of different types of security incident; be they direct costs linked to asset loss / damage or more subtle but equally damaging costs associated with the loss of company or brand reputation.

Demonstrating a more tangible ROI is, however, possible, particularly when using technology that reduces the need for manual interventions, or which allows personnel to be redeployed to other tasks. Examples can be found in solutions that not only alert personnel to suspicious behavior or intrusions, but which can also produce automated "soft" responses, such as audible announcements or flashing signage informing potential intruders that they have been detected and instructing them to leave the area.

If cameras are part of the solution, then increased efficiency can be achieved by showing the intruder that some identification data has been recorded, for example by using a screen to show a vehicle license plate, or even an image of the person themselves. Only when these preliminary measures do not produce the desired effect does the security team need to be deployed for more direct action. This phased approach to responding to alerts may be more suitable for use outside the perimeter, but they do go some way to minimizing the need for security personnel to get involved, thus freeing up resources, which has a clear benefit.

4.2 Cost evaluation

The cost estimate should be based on a Total Cost of Ownership (TCO) calculation, which includes all the costs of the solution throughout its entire life cycle: the material and human costs, the costs of studies, system installation costs, operating costs, maintenance costs, decommissioning and recycling costs. This might require a different approach by finance and procurement departments, as there might be a need to reallocate capital between operating and capital expense budgets.

5 Axis solutions

The open approach of Axis to integrating with partner solutions means that our thermal network cameras, combined with proven video analytics, enable airports to implement high-performance integrated perimeter protection solutions that are cybersecure and cost-effective throughout the system's entire lifespan.

In certain areas, where thermal sensors might not prove so effective, microwave technology (radar) is a great alternative, as it offers many of the same benefits as thermal technology. Axis radar and thermal technologies are able to differentiate between humans and vehicles, can provide speed and direction information, can integrate with PTZ cameras for effective tracking of a target, and are suitable for any part of a layered security solution — not just the perimeter. Axis radars, as well as thermal cameras, perform 24/7 with minimal false positives, as the technology is not sensitive to common triggers such as shadows, changes in lighting, small animals, raindrops, insects, wind, or bad weather. Cost savings accrue over time as fewer false positives mean less unnecessary investigative costs, as well as a smaller security team that can focus on real threats.

At a technical level, the cameras are equipped with sophisticated functions: Electronic Image Stabilization (EIS) that manages low and high amplitude movements; multiple alarm input-output ports to connect external hardware; and an advanced compression function (Zipstream) to suit bandwidth and storage requirements.

Axis cameras also feature our own ARTPEC processors, with the best capacity in the industry, allowing perimeter protection video analytic solutions to be embedded. Several cameras can therefore track multiple events occurring simultaneously in different locations. This so-called distributed technical architecture makes it possible to extend the solution to as many cameras as necessary, while eliminating investments in centralised server technology.

Four different types of events are detected, for one or more individuals or vehicles:

- Intrusion into a predefined area
- Crossing zones in a predetermined order and direction
- Conditional zone crossing
- Loitering

Axis thermal cameras also work with IP speakers to emit automatic messages upon detection, to warn would-be intruders.

The above-mentioned Axis technology can be integrated directly into software commonly used on airport platforms (Genetec, Milestone, SeeTec, Prysm, and more).

To establish which equipment is needed to enable a heightened perimeter protection solution and define the installation cost, these require both a desk study and an on-site visit. Axis supports integrators by providing design tools to plan, design, install, and manage the solutions.

Axis design tools are complimentary, and support is provided at every stage of a project – from finding the right products based on specific criteria, to planning sites, and installing and managing systems. Taking advantage of Axis tools will help the integrator run projects more smoothly and efficiently.

The tools enable the integrator to choose appropriate products and to plan optimized systems based on estimates and suggestions tailored to particular specifications. This means that the integrator can deliver the right solution faster. The tools even make it easier to keep the systems that the integrator provides more secure, because the software makes it simple to install upgrades and security patches.

6 Product references

IP thermal cameras: AXIS Q19 Thermal Camera Series

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

Analysis software: AXIS Perimeter Defender

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

External IP speakers: AXIS C1310-E Network Horn Speaker

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

IP radar: Axis radars

www.axis.com/products/radars

T10168973/EN/M4.2/2404

About Axis Communications

Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden