Perimeter protection for airports with intelligent video surveillance
Reflections on the service rendered and the return on investment

October 2019
# Table of contents

1. **Introduction** .................................................. 3  
2. **Traditional perimeter protection solutions** ............... 3  
   2.1 Physical solutions ............................................ 3  
   2.2 Intrusion detection on fences and gates .................. 3  
   2.3 Intrusion detectors outside fences ......................... 3  
3. **How to address the new perimeter protection challenges of airports** ............................................ 4  
   3.1 New intelligent video surveillance solutions .......... 4  
4. **Costs and service rendered** .................................. 4  
   4.1 Evaluation and measuring the return on investment .... 4  
   4.2 Cost evaluation ............................................... 5  
5. **Axis Communications proposal** ............................. 5  
6. **Product references** ............................................. 6
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 solutions, 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 whitepaper 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 in concrete panels. For the areas near radio navigation and communications equipment, non-metallic (or “non-magnetic”) fences are used. These fences are multi-purpose, they are a means to clearly define the airport’s boundaries, but also deter any intrusion by people and prevent access by 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 to secure large perimeters. These redirect real-time alarms to a security operator. Some suppliers offer fences that are equipped with an automatic detection solution.

These solutions, however, are not fool-proof and can produce false alarms, referred to as “false positives”. Common causes of false positives include animals, moving plants and trees, and severe weather. Without video surveillance, it is not possible to verify what caused the alarm unless personnel are able to be dispatched to investigate. Recurring 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 on distances and heights if the strict installation rules are not followed. The use of radar (microwave) 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 threat posed by these devices can be all but eliminated by the careful choice of frequency and limiting their power and consequently the effective range of the device.
3. **How to address the new perimeter protection challenges of airports**

3.1 New intelligent video surveillance solutions

The combination of video surveillance cameras and motion 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 estates.

Thermal sensors create an image using infrared radiation emitted by an object, such as a vehicle or a person and can detect activity, 24 hours a day, 7 days a week, at significant ranges, 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 the type of intrusion target and alert the operator based on a pre-set list of conditions (including direction/speed/person/vehicle). Traditional cameras are also able to do this but are reliant on using visible light, which has inherent and obvious limitations.

Depending on local laws, 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 harnessing video analytics make it possible to trigger an alarm according to set rules, for example, if a person approaches within 50 metres of the fence, followed by a higher alarm level if that same person breaches a 10 metre zone, or is loitering for 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 the ability for a thermal based solution to provide effective long-range monitoring in any lighting and harsh weather is why such 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 in modern times can range from protestors to terrorists, while adhering to any relevant compliance requirements.

A converged approach to security that includes inputs and considerations from other departments, such as IT and operations, is fast becoming best practice. Additionally, and of relevance to airports with large areas of restricted access, there is a need to involve those with experience in conducting the civil engineering requirements as early as possible. Historically a good starting point for the perimeter would always 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.

Demonstrating a Return on Investment of a security solution designed to prevent an incident is notoriously difficult. This is predominantly 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 due to asset loss or destruction or more subtle but equally damaging costs associated with loss of company or brand reputation.
However, demonstrating a more tangible ROI is possible, particularly with certain technology capable of reducing specific manual activity or allow personnel to be redeployed to other tasks such as improving the passenger experience. Examples can be found in solutions that not only alert personnel to suspicious behaviour or intrusion, but can also produce an automated soft response, such as an audible announcement or flashing signage informing the potential intruder that they have been detected and instructing them to leave the vicinity.

If cameras are incorporated into the solution, increased effectiveness can be achieved by showing the intruder some degree of identification, such as an electronic screen showing the license plate has been captured or even an image of the intruder. Only when this does not have the desired effect need the security team be deployed to investigate or take more direct action. This phased approach to responding to alerts might be more suitable for beyond the perimeter, but they go some way to minimize the requirement for security personnel to get involved and freeing up man hours which has a clear benefit.

4.2 Cost evaluation

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

5. Axis Communications proposal

Axis' open approach to integrating with partner solutions means that its thermal network cameras, combined with proven video analytics, enable airports to implement high-performance integrated perimeter protection solutions that are cyber secure and cost-effective across the whole life time of the system.

In certain areas, where thermal sensors might not provide value, microwave technology (radar) is a great alternative, able to offer many of the same benefits as thermal. The Axis radar technology is able to differentiate between humans and vehicles, provide speed and direction information, 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. Similar to thermal, radar technology performs 24 hours a day with minimal false positives as it is not sensitive to common triggers such as moving shadows or light beams, small animals, raindrops or insects, wind, and bad weather. Cost savings are made over time as fewer false positives mean lower unnecessary investigative costs and a reduced security team as they 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 in order to connect to external hardware; and an advanced compression function (Zipstream) to suit bandwidth and storage requirements.

Axis cameras also feature Axis' own ARTPEC processors with an industry leading capacity, 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, whether for one or more individuals or vehicles:

> Intrusion into a predefined area
> Crossing zones in a predetermined order and direction
> Conditional zone crossing
> The presence of loitering
Axis thermal cameras also work with IP speakers to emit automatic messages upon detection to warn any would-be intruder.

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

To establish the equipment needed to enable a heightened perimeter protection solution and define the installation cost, both a desk study and an on-site visit are required. 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, 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 plan optimized systems based on estimates and suggestions tailored to particular specifications. This means that they are able to deliver the right solution faster. The tools even make it easier to keep the systems the integrator provides more secure because the software makes it simple to install upgrades and security patches.

For more information, please contact Lucas Young (lucas.young@axis.com).

6. Product references

IP thermal cameras: AXIS Q19 Series

Analysis software: AXIS Perimeter Defender

External IP speakers: AXIS C3003-E Network Horn Speaker

IP radar
Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems. Axis has more than 3,000 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website www.axis.com.