WHITE PAPER

Perimeter protection with intelligent surveillance

A study of sensor options, applications and key considerations to ensure a future-proof security solution across a range of industries

July 2021

AXIS COMMUNICATIONS

Table of Contents

1 **Summary** 3

2 **Introduction** 3

3 **Perimeter protection solutions** 4

- 3.1 Physical solutions 4
- 3.2 Intrusion detection on the physical perimeter 4
- 3.3 Other intrusion detection sensors 4

4 **Video-based solutions** 4

- 4.1 The application of video cameras 4
- 4.2 Thermographic video surveillance solutions 5
- 4.3 Visible light cameras 5
- 4.4 Video content analytics 6

5 **Costs** 7

- 5.1 Evaluation and measuring a return on investment 7
- 5.2 Cost evaluation 8

6 **Axis Communications' proposal** 8

1 Summary

A fence is often a fundamental component of the 'outer layer' of a site's security, and it can act as a barrier, as a screen, or as a deterrent, to both people and animals. Other features can be incorporated to enhance the fence's effectiveness, as any physical barrier can only delay or hinder an intrusion.

Various types of detectors are used alongside fences. Cable-based detectors can follow the route of the fence, and radar (microwave) sensors, infrared barriers or lasers can be positioned at strategic locations.

All types of detectors can produce false alarms, as caused by, for example, animals, moving plants and trees, and inclement weather. There may also be other constraining factors, such as frequency clashes when using microwave sensors, or physical limitations in the installation environment.

Cameras provide an obvious benefit for those wishing to monitor large areas or multiple locations. Modern networked video solutions combine on-camera computer processing and artificial intelligence. The inherent scalability, effectiveness and deterrent nature of the technology means that video cameras are potentially a highly cost-effective addition to a security system.

Although cameras and motion detection software have expanded the range and capabilities of perimeter protection, these solutions can be limited by an inability to detect in adverse weather conditions. Thermal cameras, when properly calibrated and coupled with video analytics, provide effective surveillance and monitoring, unaffected by lighting conditions and virtually unhindered by extremes of weather.

Video analytics have evolved significantly over time and are now commonplace, even in cameras aimed at the home security market. Analytics can reduce storage requirements by only recording the video that contains activity of interest. By processing much of the recorded video within the camera itself, the load on the network is significantly reduced, as only relevant video is streamed from the cameras. This has obvious benefits in a control room scenario.

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.

A converged approach to security that includes inputs and considerations from other departments, such as IT and operations, is fast becoming best practice. This includes a need to include those persons handling the engineering as early as possible.

Demonstrating the Return on Investment (ROI) of a security solution designed to prevent an incident is notoriously difficult. This is mainly due to of a lack of potential revenue to measure against the cost. Demonstrating a more tangible ROI is possible; examples include solutions that not only alert personnel to suspicious behavior or intrusion, but which also produce automated responses.

2 Introduction

Electronic perimeter protection solutions have traditionally been the preserve of high-security government and commercial sites, or of the very wealthy. With advancements in technology, a more competitive marketplace and the consequential reduction in costs, relatively hi-tech solutions are now available to many more.

So what does a modern perimeter protection solution consist of? What is the technology at work and how can it provide both reassurance and genuine protection?

This white paper examines some of the current sensor-based options for protecting a perimeter and provides an insight into the technology behind the solutions.

3 Perimeter protection solutions

3.1 Physical solutions

Physical solutions are often a fundamental component of the 'outer layer' of a compartmentalized approach to securing a site, which typically comprises a perimeter fence, often constructed of wire or welded mesh, in welded or concrete panels. A perimeter fence serves many purposes, one of the main ones being to present a physical barrier that will delay or prevent intrusions. A fence can also prevent surveillance by screening an asset; and it serves as a deterrent and prevents animals from entering. Features such as anti-climbing devices, designated vehicle access routes, anti-crossing devices, and fence screens can also be incorporated to enhance a perimeter fence's effectiveness.

However, any physical barrier will invariably only delay an intrusion. Therefore, the perimeter should also be equipped with automatic intrusion detection technology, which is capable of providing verifiable real-time alerts, location data, target tracking and the ability to package the evidence and data for post-incident investigation.

3.2 Intrusion detection on the physical perimeter

Various types of cable 'detectors' are often used to secure extended perimeters. These cable-based detectors are usually buried in the ground or mounted on the fence, they follow the route of the fence, and don't need to be in straight lines. They also provide coverage around corners and in **dead-ground areas**. Some suppliers offer fences equipped with automatic detection solutions.

As with any detection solution, cable-based detectors can produce false alarms, referred to as 'false positives'. Common causes of false positives include animals, moving plants and trees, and severe weather. Cable-based solutions work best when augmented with video surveillance. Video can be used to not only verify an intrusion, but also to ascertain the cause of an alarm. A cable-based solution will only be able to provide an alert for the intrusion itself; it can't provide information on the number of intruders or any other details required to prepare a response.

3.3 Other intrusion detection sensors

Other intrusion detectors, such as radar (microwave) sensors, infrared barriers or lasers can be positioned at strategic locations around the perimeter. Again, these technologies can be constrained by issues such as false positives, and limited detection capabilities with regards to distance and height, if installation rules are not correctly followed.

The use of radar on the perimeter can be particularly problematic in an environment that uses other electronic devices. These may operate on the same frequency and spectrum, and while a careful choice of frequency or reduction in power may reduce interference, it will also hamper the effective range of the device.

4 Video-based solutions

4.1 The application of video cameras

The stand-alone legacy CCTV technologies of the past bear little resemblance to the hi-tech network camera solutions available today. Modern network solutions are capable of combining both in-camera

computer processing and artificial intelligence. This level of technology, however, has only recently been made available and is still in its infancy.

Cameras provide an obvious benefit to those wishing to monitor large areas or multiple locations. The inherent scalability, effectiveness and deterrent nature of the technology means that video cameras are potentially a highly cost-effective addition to a security system.

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. Solutions that harness video analytics make it possible to trigger an alarm according to set rules. For example, an alarm sounds if a person approaches within 50 metres of a fence; a higher level of alarm might be triggered if that same person continues to loiter, or enters the 10 metre zone.

4.2 Thermographic 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. However, the effectiveness of video can be severely limited by its inability to detect in adverse weather conditions.

The increased availability of thermal camera technology has led to the prominence of their use on the perimeter. Thermal (or thermographic) cameras, when properly calibrated and coupled with video analytics, can provide effective surveillance and monitoring, unaffected by lighting conditions and virtually unhindered by extreme weather. Sensors using thermal technology provide superior contrast compared to a typical visible light camera and are consequently beneficial for perimeter protection due to vastly improved intrusion detection capabilities.

Thermal sensors create an image using infrared radiation emitted by objects such as vehicles or persons. When combined with video analytics, modern thermal cameras with sufficient processing power can distinguish between different types of intrusion target and can alert the operator based on a pre-defined list of conditions. These might include the direction and speed of a person or vehicle. Traditional cameras are also able to do this, but they need to do so using visible light. These cameras are explored in the following section.

4.3 Visible light cameras

All standard visible light surveillance cameras need either natural or augmented lighting to provide images. Lighting to support video surveillance is an area of expertise in its own right and separate papers have been written on this important subject. However, we still need to reiterate the obvious yet critical point that standard cameras need visible light. Light can be a challenge in any environment, with obvious effects as light quality changes. Something not always considered or understood, particularly by those specifying the solution, are the effects of the weather.

Thermal cameras have their benefits, but this is not to say that thermal cameras should or can be a direct replacement for the visible light camera – far from it. These two technologies work best when integrated in the same solution. Traditional cameras cannot detect objects at the ranges of thermal cameras; but thermal cameras cannot provide the forensic detail provided by visible light cameras. The two technologies are often combined, with the thermal camera providing the detection alarm and the forensic benefit of the visible light camera providing both evidence and target tracking.

4.4 Video content analytics

Network video surveillance has brought unprecedented scale to security operations. An effective permission hierarchy enables controlled video access, distribution and storage across a theoretically unlimited number of stakeholders. One technological advancement in particular is bringing even greater levels of scalability - video analytics.

Video analytics have evolved significantly over time, not least due to the development of IP camera technology. This can be evidenced in cameras aimed at the home security market, many of which now incorporate some level of analytic function, enabling them to, for example, detect motion in the scene. Additional functionality may come 'bundled' with a camera, including cross-line detection, moved objects, or even people counting.

Video analytics can remove the requirement for storage space by only recording video that contains activity. Also, by processing as much of the recorded video within the camera itself (known as 'intelligence at the edge'), the load on the network is significantly reduced as only relevant video is streamed from the cameras. This has obvious benefits in a control room scenario, with a security operator only having to examine video when an alert is received, a major improvement for both the security operator and the organization's operational efficiency.

There are two broad categories of system architecture for implementing video analytics: centralised and distributed. In centralised architectures, video and other information is collected by cameras and sensors and sent to a central server for analysis. In distributed architectures, the edge devices (network cameras and video encoders) themselves are capable of processing the video and extracting relevant information. Analysis at the edge removes the requirement for dedicated analytics servers, and as compression is only utilized when transferring video data to a central server, analysis can now be performed on the uncompressed video feed. The result is a much more cost-effective and flexible architecture. In fact, the same servers that could typically process only a few video streams due to the processing power required, can now handle hundreds of video streams when much of the processing is carried out in the cameras.

4.4.1 Processing speeds and GPUs

Although Gordon E Moore's accurate prediction (aka Moore's law) of exponential improvement in processing speeds and capacity has been forecast by some leading tech companies to slow down in the near future, the current increase in power combined with the reduction in size has meant that camera manufacturers and developers can change the way processing power is harnessed.

Up until recently, any additional processing capacity was utilized to improve image quality, bringing increased resolution and more efficient video compression. For the time being, however, the market seems to have almost reached a plateau in its demand for ever greater image resolution. Consequently, manufacturers are now using the processing power to provide levels of intelligence never before seen on the edge. In many cases this means that powerful server-based video analytics can now benefit from being processed in the camera.

The smaller and faster characteristics of modern processors means that cameras are able to accommodate Graphic Processing Units (GPUs), providing parallel processing capabilities, and open up new opportunities and analytic possibilities. This new capability has resulted in software developers switching their attention to providing newer versions of existing and proven server-based analytics in edge-based variants, helping drive the demand for more intelligent cameras, capable of delivering value far beyond just security and video surveillance.

4.4.2 Deep learning and artificial intelligence (AI)

GPUs have enabled a leap in analytic performance at the edge, but demand is growing for other types of technology to be applied in surveillance settings, providing features such as people counting and occupancy management. Developments in AI and machine learning have led to Deep Learning Processing Units (DLPU) being integrated into cameras, which is proving to be a game changer.

A DLPU is purpose-built for the wider application of deep learning analytics. Analytics based on deep learning can provide superior accuracy for detection and classification, as the algorithm is effectively trained on what a set of prescribed objects looks like. This means that an intrusion detection solution on a perimeter can be set up to only raise alerts for very specific objects and scenarios; an advanced version of If-this-then-this (ITTT).

In some cases, only part of an object might be visible, such as the rear bumper of a car, but the system analytics system will still recognise and identify it. At the time of writing, and despite some claims, most proven solutions on the market are limited to identifying and discriminating between people and vehicle types. However, examples of camera-based analytics models capable of more detailed discrimination, such as the color of the clothes a person is wearing, are at an advanced stage of testing.

These advances in technology could potentially lead to highly targeted detection systems, able to identify and differentiate between employees, customers, members of the public or potential threats. From a security perspective, advanced analytics in a setting with well-applied physical security can only result in an even more efficient and accurate system for detecting and preventing crime. The evolution to the next stage of capability might not be such a long way off.

5 Costs

5.1 Evaluation and measuring a return on investment

As with any security measure, be it from a vulnerability or resilience perspective, evaluation of a perimeter protection solution should be both appropriate and proportionate. As always, the threat needs to be the primary consideration, which for almost any sizable corporation or government site in modern times can range from accidental trespassers to protestors or even terrorists.

A converged approach to security that includes inputs and considerations from other departments, such as IT and operations, is fast becoming best practice. This includes a need to involve those with experience in engineering requirements, and they should be engaged as early as possible. When considering the measures to be applied, a good starting point historically for the perimeter would always have been the more traditional measures, which typically deter and delay a potential intruder. Only then would the security designer 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 the Return on Investment (ROI) of a security solution designed to prevent an incident is notoriously difficult. This is predominantly due to a lack of potential 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 less immediate but equally damaging costs associated with the loss of reputation.

However, demonstrating a more tangible ROI is possible, particularly with certain technologies capable of reducing specific manual activity or allowing security personnel to be redeployed to other tasks. Examples can be found in solutions that not only alert personnel to suspicious behavior or intrusion, which but can also produce an automated soft response. These might include IP audio systems that can deliver

pre-recorded announcements, or illuminated signage informing a potential intruder that they have been detected and instructing them to leave the area.

If surveillance cameras are incorporated into the solution, increased effectiveness can be achieved by showing the intruder some evidence of their identification, such as a screen showing that their license plate has been captured or even an image of the intruder. Only when this does not have the desired result is it necessary for the security team to be deployed to investigate or take more direct action. This phased approach in response to alerts might be more suitable for use beyond the perimeter, but will help minimise the need for security personnel to get involved at an early stage, thus freeing up man-hours for a clear efficiency benefit.

5.2 Cost evaluation

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

As with any tangible asset, the organization will need to know the useful life of the perimeter detection solution. Security and IT managers can help their colleagues in finance by explaining and demonstrating how procuring the right technology as a platform for future solutions will save money. A characteristic of advanced intelligent surveillance devices is that they are, to some extent, inherently future-proof. That is to say, devices with suitable processing power are capable of repeatedly taking advantage of technological advancements over time, most notably through processing analytics based on AI and machine learning.

6 Axis Communications' proposal

Axis' open approach to integrating with partner solutions means that its networked sensors, combined with proven video analytics and harnessing AI, allow customers to implement high-performance, integrated perimeter protection solutions that are cyber-secure and cost-effective across the entire enterprise and for the system's entire lifetime.

Where thermal sensors might not be appropriate, microwave technology (radar) is a great alternative, able to offer many of the same benefits as thermal, with potentially fewer false positives. Axis radar technology benefits from the same machine learning and deep learning as the more advanced surveillance cameras. Axis radar units can accurately detect, classify, and track people and vehicles with almost zero false alarm rates.

Radar technology performs 24/7, and is virtually unaffected by common triggers such as moving shadows or light beams, small animals or insects, or adverse weather conditions. This results in a highly cost-efficient operation, ensuring security personnel can focus on genuine confirmed threats. Radar can also provide the speed of an object, enabling the accurate calculation of point of contact or even for enforcing speed limits.

A solution's performance is often the first part of any request for information (RFI) or market analysis questionnaire. Axis cameras feature Axis' own ARTPEC processors, with industry-leading capacity, allowing some of the most advanced perimeter protection video analytics solutions to be embedded into the camera (on the edge). Crucially, this also provides assurance that the solution is harnessing the power of in-house technology and not of third-party components.

This 'on the edge' intelligence means that 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.

With the UK government's approved AXIS Perimeter Defender (APD), 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
- The presence of loitering

APD can provide more than just an intrusion alarm and corresponding video. It also provides metadata that can be utilized to display an overlay on the video, showing the boundaries and trajectories of moving persons and vehicles. For a more integrated approach, Axis cameras (visible light or thermal) also work with IP speakers to broadcast automatic messages upon detection, potentially as a standalone solution. This type of automated warning will enable an 'escalation' of measures and countermeasures, important in determining an intruder's intent and any subsequent response required.

APD can be integrated directly into the software commonly used on enterprise platforms (e.g. Genetec, Milestone, Seetec, Prysm, Qognify and more).

Axis provides complementary design tools to help with post-survey planning, and support at every stage of a project, from finding the right products based on specific criteria to accurately calculating storage requirements, installing the technology and managing the systems. Taking advantage of Axis tools will help consultants plan and estimate, and an integrator to manage projects more smoothly and efficiently. These tools even make it easier to guarantee the security of the installed system because the included software makes it simple to install upgrades and security patches.

As threats and countermeasures evolve, one critical thing remains constant; the integrity and security of the perimeter. The perimeter is a fundamental consideration for those implementing an organization's duty to provide a safe and secure environment for staff, visitors and members of the public. This paper is intended to promote the benefits to organizations of an integrated technology approach when planning perimeter security. It also highlights the fact that security technology investment should be supported by a demonstrable ROI. In all cases, understanding current relevant technology capabilities as well as an appreciation of future trends is a sound operational security and procurement approach for any security practitioner, no matter their department, title or industry.

Product references

IP thermal cameras:

AXIS Q19 and more www.axis.com/en-gb/products/thermal-cameras

Analysis software:

AXIS Perimeter Defender

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

External IP speakers:

AXIS C1310-E www.axis.com/en-gb/products/axis-c1310-e

IP security radar:

T10169467/EN/M2.2/2107

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