White paper

Drawing the line

Network video for flexible and
versatile perimeter protection

AXIS® COMMUNICATIONS

Table of contents

1. Introduction

Not knowing what is happening to your property when you are away is worrisome and discomforting. Yet, knowing that something has happened, but not exactly what, can be just as frustrating, sometimes even worse. Network video surveillance offers versatile perimeter protection that allows you to find what's going on around your premises and why, and thereby enabling resourceful and cost effective protection of your assets.

2. Traditional measures for perimeter protection

To safeguard against trespassing, theft and vandalism, business owners as well private households invest in various perimeter protection measures. Traditionally, these measures relied on technologies such as short-distance radar, lasers, ground sensors, motion sensors or motion-sensitive fence wires.

They all perform well, and can, under many circumstances capably detect an intrusion. However, all of these systems have an obvious and significant limitation: they cannot distinguish between real and false alarms. So for every alert, someone – i.e. the homeowner, business owner or the security company providing the services – has to decide whether or not a patrol should be dispatched to the area. Not until an inspection is carried out can it be confirmed if there has been an actual breach of the perimeter, and if this breach is a threat that needs to be dealt with, or whether it was caused by something harmless, e.g. an animal.

Such procedures tend to be rather time-consuming and will – especially if the false alarms are frequent enough – eventually lead to more lax or even dropped security checks. Consequently, the whole operation runs the risk of becoming very expensive without providing any peace of mind.

3. Network video for a clear picture and strong decision support

With network video cameras, on the other hand, it is possible to build an intelligent and reliable surveillance system for perimeter protection. A vast range of products from the leading supplier makes such IP-based systems very versatile and high performing, especially in difficult lighting environments and in varying and demanding weather conditions.

Clear and crisp images facilitate detection and identification of objects, people and incidents, thus making it easier to separate true alarms from false alarms and other incidents that don't require any measures to be taken. Automated solutions and video analytics software can further reduce the need for monitoring staff.

3.1 Detect – verify – act: How it works

Basically, the main objective for perimeter protection is to detect a threat or an intrusion at the earliest possible stage. However, areas where valuable assets are sometimes kept, for instance rail yards, bus depots, car parks or harbors can pose a significant challenge for security managers. The sheer size of these places can be a problem. Lighting conditions can also present a problem, especially during nighttime if there is little or no electric lighting available.

3.2 First line of defense – thermal network cameras

Modern thermal network cameras are very sensitive and accurate. They are unrivaled when it comes to detection, making them ideal in a first line of defense. Once a suspicious event has been detected, the thermal camera can be configured so that it automatically directs a PTZ (pan/tilt/zoom) camera to the right place. Working in parallel, these two camera types form an unbeatable combination.

As opposed to day/night cameras, which use the near-infra red spectrum of light, thermal cameras do not require any light at all to operate. Instead, these cameras are able to detect a person or an object by visualizing the thermal radiation they emit. This capacity makes the cameras highly functional in complete darkness as well as in fog, snow and other challenging conditions. Less apparent is their usefulness in broad daylight. Thermal cameras are nevertheless also very efficient when it comes to discovering people or objects that are obscured by complex backgrounds or who hide in deep shadows. Another benefit is that strong lights or laser pointers cannot interfere with them.

3.3 On top with PTZ domes and fixed cameras

With thermal network cameras, operators can detect suspicious activity around the clock. However, after detection must follow verification before any decision on further actions can be taken.

PTZ cameras are very adaptable and can enable an operator to get on top of a situation very quickly. After an alert, he can pan and tilt the camera by remote control and get an overview of the area in question. From there it is easy to zoom in on details. State of the art network cameras deliver sharp images with very high resolution enabling facial identification or license plate recognition even at very long distances.

There are many situations where surveillance video with color is an important factor for successful identification. Special low-light technology that reduces noise and maintains colors even in very dark conditions is therefore a useful capability that greatly enhances the user's possibility to effectively recognize and identify people, vehicles and incidents.

A visual close-up also helps the security operator to further analyze the situation at hand. Is the person that caused the alarm an unwanted intruder with possible ill intent? Or is it a visitor who has come astray or is it simply somebody who is an authorized staff member?

The whereabouts of detected trespassers can be followed with a remotely operated PTZ dome or well-placed fixed cameras while an employee or a guard patrol is guided to intercept the perpetrator. Saved video of an intruder's movements and activities can later prove valuable evidence in a trial.

4. Scalable, flexible and cost efficient

The descriptions above imply large surveillance systems covering huge areas with plenty of security personnel and a well-equipped command center. But neither technology, nor price, put network cameras out of reach for smaller businesses or even private homes. On the contrary, with analytic software and other clever applications a video surveillance system can be more or less automated and very cost effective.

4.1 Automation – detection without eyes

Network video allows for distributed intelligence, i.e. units at the edge capable of processing video and extracting relevant information. This requires less bandwidth and reduces the need for storage since only relevant video footage is downloaded onto the server. Even small and rather basic systems provide the high quality images needed to enable advanced features such as video motion detection, virtual fence or cross line detection. Compared to a radar or laser system that is typically installed on the inside of a fence, a network camera can be configured to sustain an alarm trigger outside of the fence and thus give an earlier warning.

Large systems allow even more advanced configurations and functionalities. For example: Object filtration which reduces the number of false alarms by only reacting to objects that fulfill certain, predetermined criteria, such as size and speed etc. Similarly, conditional alarm requires a number of rules to be fulfilled before the alarm is triggered. Another example of a useful application to minimize false alarms is masking area, which is a zone within the camera's field of view where events don't trigger alarms.

4.2 Automatic notification

When an alarm is triggered, a real time notification is automatically sent by e-mail. Using a remote viewing app, the receiver can then see a live stream from the camera or a recording of the triggering event. Based on this visual information, it is easy to go ahead and decide on the appropriate action.

IP-based systems are flexible and scalable as well as being possible to integrate with other security technologies, such as access control and motion sensors etc. Relying on open industry standards also facilitates the development of a wide variety of third party applications.

5. Conclusion

Network camera surveillance for perimeter protection enables you not only to detect a possible intruder at an early stage, but it will also help you to verify the extent and severity of a breach as well as providing essential visual information to adopt an appropriate response. Furthermore, by checking video streams, it is easy to distinguish false alarms from serious intrusions.

The versatility of network cameras, in combination with many available applications and video analytics software, makes the system flexible, scalable and cost efficient. Finally, avoiding all the work, stress and problems that are caused by misinterpreted alarms will also pay dividends – if nothing else, in the form of a greater peace of mind.

A network camera surveillance system doesn't leave you in the dark.

64698/EN/R1/1507

About Axis Communications

Axis offers intelligent security solutions that enable a smarter, safer world. As the global market leader in network video, Axis is driving the industry by continually launching innovative network products based on an open platform - delivering high value to its customers and carried through a global partner network. Axis has long-term relationships with partners and provides them with knowledge and ground-breaking network products in existing and new markets.

Axis has more than 1,900 dedicated employees in more than 40 countries around the world, supported by a network of over 75,000 partners across 179 countries. Founded in 1984, Axis is a Sweden-based company listed on NASDAQ Stockholm under the ticker AXIS.

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

AXIS® COMMUNICATIONS