

SENSE AND VISION

Sensor-led visual verification is becoming essential for businesses of all sizes, according to OPTEX

INTRUDER DETECTION

For decades, intrusion detection in residential and light commercial premises has been performed without the use of CCTV or visually verifying the cause of an alarm. Intrusion sensors were connected to alarm panels which activated when the sensors were triggered. But all of this is changing. Even when an alarm is known to be genuine, thanks to the reliability of the sensors installed, there is still the desire to know who/what has caused the alarm and whether there is an urgent need to respond. Visual verification is becoming a 'must' throughout the security industry, with everyone steadily moving away from 'blind' intrusion alarm systems to ones that can be visually verified.

The question some are asking now, however, is does it make the sensor redundant? Can the detection, lighting and visualisation be achieved by a single piece of equipment and specifically the camera?

As much as camera technology and video algorithms have evolved, there is still both a risk and limitation in using a single technology to do everything. We have seen in the last few years, leading camera manufacturers investing in or acquiring sensor technologies. Key video software companies have also been emphasising the fact that video analytics is not a panacea and other technologies are better placed to provide reliable detection and therefore a reliable trigger to the video component.

Detection in difficult lighting conditions

One of the benefits of modern sensor-led detection installations is that they don't need light to perform. The same cannot be said for cameras.

By definition, a video device cannot process what it doesn't see. The security market has seen the development of low light cameras, as well as video analytics featuring additional background filters. Yet camera manufacturers themselves warn against the limitation of detecting motion in difficult lighting conditions. This ranges from badly illuminated corners or areas on the scene, flashing/flickering lights, headlights, moving shadows etc all of which impact camera performance. Poor lighting affects the camera quality but also lighting in the wrong places can produce glare and shadows making the video motion detection less stable.

"As much as camera technology and video algorithms have evolved, there is still both a risk and limitation in using a single technology to do everything."

Physical intrusion sensors have been developed around a number of different technologies such as passive or active infrared, microwave, LiDAR, Radar and fibre optics, but the common characteristic of them all is that they don't need light to detect.

In an outdoor environment where lighting conditions are constantly changing, using physical sensors will considerably reduce the risk of false alarm or missed detection.

Our sensors incorporate the ability to self-adjust their

sensitivity thresholds under varying light conditions. They also have built-in algorithms to automatically increase/decrease the threshold at sunrise and sunset, two of the most difficult lighting scenarios for any detection system to discern individual objects.

Detection speed

In simple terms, the more a device has to multitask the more time it takes to process a response. A camera has first to process a number of frames and pixels to be able to analyse the scene, filtering information, recognising and identifying shapes and their movement, all of which takes time.

Depending on the algorithms and processing power used inside a camera, the time to detect movement and generate a response will vary. To cut down on processing time, some video analytics will deploy a variety of predictive algorithms, but these are not wholly reliable. What we can say is, even with modern processors, the whole video image processing affects the speed and reliability of detection and some detection can be missed. For many customers, missing an event is considerably more dangerous than a nuisance alarm. The ideal scenario is to have no missed detection and no nuisance alarms.

If we take the example of our sensors, we are using algorithms to process data and eliminate noise but without using any predictive elements. This eliminates the risks associated with guess work and improves reliability. Our sensors are also not having to process data such as colours, nor are we trying to process high definition detail.

Intrusion sensors are there to perform one single task: detecting. Modern and advanced

sensors feature digital processing and analytics which also require some time to process but it isn't as complex as analysing pixels.

Detection range

Detection range is a key element of system design as it determines the different alarm zones from pre-warning to critical. What is important is to make sure that the detection ranges are consistent throughout the day and in varying weather conditions.

"By adding a reliable outdoor sensor as a trigger to the camera, the level of nuisance alarms will drop dramatically."

If a detection range has been specified at 30m for instance, it is critical that detection is as accurate at 30m as it is at 2m or 15m.

Video devices will use depth of field and define how many pixels an object has within the ranges defined. In the last ten years, significant progress has been made on that front and higher end cameras have the ability to be configured for variable object size depending on the distance. Mid- to low-range cameras usually don't have this feature and therefore don't capture motion with accuracy at longer ranges. The depth of field can also be shortened by decreasing light intensity, cameras might not see as far at dusk as during daytime.

Our sensors are designed to capture motion consistently throughout the detection range. For our PIRs and active beams, this is achieved through the design of the lenses. Our LIDAR series has a resolution of 0.25 degree enabling a very dense and accurate detection at the boundary of the detection range.

Benefits of sensor-led visual verification

The residential and light commercial markets are typically using mid- to low-range cameras, which will be more likely to trigger false alarms, especially if used in an outdoor environment. By adding a reliable outdoor sensor as a trigger to the camera, the level of nuisance alarms will drop dramatically. It will cut down the constant alerts regardless if we are talking of self or centrally monitored intrusion systems. It has never been so easy to combine sensors and video as most security systems can work with multiple inputs. Alarm panels have evolved into an alarm and video gateway, NVRs can take events from sensors to drive cameras and an IP Bridge can be utilised to connect existing cameras with the alarm system.

It is a real opportunity with a very reasonable budget to improve the reliability of intrusion detection for that sector and also give the option to extend it to the outside of the building.

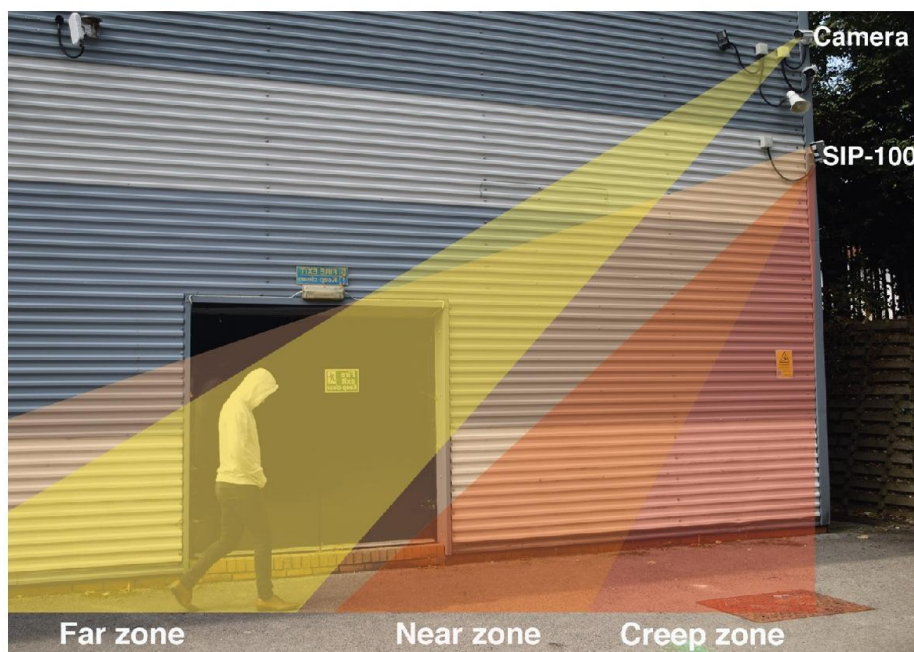
Commercial and high-end security environments

For commercial and higher security sites, there are a number of critical points to consider. Fundamentally,

not missing alarms is crucial, as well as keeping nuisance alarms as low as possible. Avoiding single points of failure and disruption caused by constantly having to reconfigure the systems to adapt to changing environments are also important factors that need to be assessed.

Using high-accuracy sensors together with good quality cameras managed by a high-performance video management system will give the best of breed to the end users. For all the reasons outlined earlier, there are clear benefits in an outdoor environment for using sensors as the first line of defence in detecting intrusions. It decreases the risk of missed alarms, adds a level of redundancy and reduces the number of nuisance alarms. Once installed and set up correctly, intrusion sensors rarely need reconfiguring, except if an environment changes (for example because a bush has grown). Video analytics, however, require a more regular change of settings.

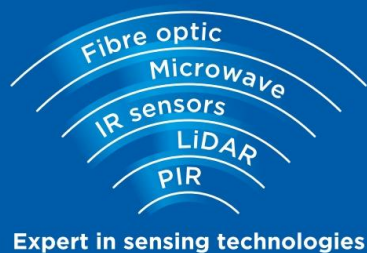
In the last few years we have worked in close cooperation with video manufacturers and we have seen the true value of bringing the two technologies together. It is now time that installers realised the benefits that such cooperation can bring to their business and their customers.





DON'T WASTE TIME ON EMPTY THREATS

Get the power of sensor-led visual verification



Empty threats waste time and missed threats could have disastrous consequences.

For enhanced security, it makes sense to bring the power of two technologies together. Our intelligent sensors can detect without being influenced by light or weather conditions and integrate with video systems to provide visual verification. Because vision can't do it all, it makes sense to have sensor-led visual verification.

For more information visit www.optex-europe.com