FENCING LESSONS

Faced with securing extensive sites and an evolving threat spectrum, port operators are having to get smarter in their selection and deployment of barriers and sensors. **By Joe Charlaff**

Large ports, like the Port of Los Angeles Long Beach, must contend with extended perimeters. (Photo: NOAA)

Perimeter security is a major issue for any seaport or airport. The threats are numerous, with the most obvious and potentially most damaging being the risk of terrorist incursion.

Seaports, both freight and cruise line facilities, face a number of distinct challenges in this respect. Because they include both a sea side that cannot be fenced and a land perimeter, security must account for these two vastly different terrains.

Given that seaports cover large areas, security personnel are unable to monitor all locations at all times. As terrorism has become a major phenomenon worldwide, critical infrastructure is subject to a greater danger from attacks than ever before.

Getting physical

Perimeter security can include video detection, intrusion detection, access control, fencing/gates and barriers/bollards. The type of systems and technologies deployed will depend on the likely intrusion risks, which can range from vandalism or protests by activists, to criminal theft, espionage and the aforementioned terrorism.

While there has been huge investment in CCTV and electronic systems, physical perimeter security has not always received the same attention. This is beginning to change, however, as perimeter protection systems become embedded into integrated strategies.

Securing the landside perimeter of ports is difficult due to their typically large size. Facilities located in urban areas allow terrorists a densely populated zone in which to hide while infiltrating or escaping the port. The high volume of trucks entering and departing such facilities poses a threat. Exiting vehicles may contain weapons of mass destruction or operatives who are to infiltrate a surrounding metropolitan area.

Strategic installations and economic infrastructure along borders, at sea and underwater have been targets for hostile states, terrorist organisations and other elements, with threats potentially being airborne, surface or subsurface.

The security community has been constantly searching for innovative technological means to monitor and protect strategic assets such as electricity grids, water supplies, oil refineries, vital industries, chemical plants, transportation networks, telecommunications, ports and airports, etc.

Going in circles

Speaking to *IMPS*, Alon Globus, marketing manager of RBtec, explained the company's strategy, technologies and what he terms the 'circles of security'.

He said that the first layer monitors the areas outside of the fence, using optical sensors and surveillance systems, such as those seen near border crossings in the Middle East. These systems trigger responses by security personnel. ▶

Whether soldiers or port security officers, the concept is the same.

'If you have CCTV cameras with an analytic system, the moment it recognises a movement, it will open the main screen and the observer will see what is going on,' said Globus.

Meanwhile, the fence itself can often have a motion sensor integrated into its structure. Products such as RBtec's SL-3 Ironclad can be mounted and provide additional security layers around the site.

A recent theft of weapons from an Israeli military base in the south of the country highlighted the need to provide comprehensive perimeter security capabilities.

'Had there been a fence with an intrusion detection system, plus an access control system having a logbook showing who entered at what time, the thieves would probably not have succeeded,' Globus said. Early detection of an attempted intrusion is essential, as is determining the exact zone of the fence where it takes place.

'We divide the fence into zones in order to have full control and the same applies to borders. Codes are assigned to the zones enabling swift identification.'

The security procedure is initiated as soon as the alert sounds, automatically opening cameras, and triggering sirens and spotlights on the fence, which will temporarily blind any intruder and buy time for the security forces to take action. In sensitive areas, unmanned systems can also be deployed.

RBtec's Marinet system was designed to provide a solution for waterways and underwater areas that require a smart barrier for perimeter protection and reduce false alarms. For ports, and naval bases in particular, one danger is from scuba divers who can enter the harbour and place mines on ships.

'An underwater fence is a beginning, but if you don't have a detection system you will not know that something is happening under the water,' Globus emphasised.

The system is a criss-cross array of electronic fibre-optic net reinforced with Kevlar and steel cable, which is designed to prevent any undetected breach from occurring. The Marinet also functions as a physical barrier to protect waterside perimeters from dangers such as speedboats, divers or floating explosive packages.

The system will trigger an alert and allows for tides, underwater currents, wind and water salinity which can cause damage to the system.

Turnkey technology

Joseph Nissan, business development director of Israel-based wireless communications company Radwin, spoke to *IMPS* about his company's solutions for landside perimeter security.

'We work with system integrator companies that are providing turnkey solutions to armies and agencies, responsible for securing the country's border from terrorists, illegal immigration and drug smuggling. They

Detection systems and sensors are integrated into the perimeter fencing to provide enhanced detection and localisation. (Photo: Optex)

The SL-3 sensor installed on site. (Photo: RBtec)

typically need to have a portfolio of sensors as well as communications infrastructure to deliver the sensor traffic to a command centre and back to the field to a mobilised patrol of troops.'

Radwin has developed a mobile system called FiberinMotion that is customised to address the specific challenges of border security applications. This is already operational on several borders, providing high-resolution mobile video transmission to and from patrol vehicles, both manned and unmanned.

One prominent border is of course that of the US. The country has more than 19,000km of coastline and hundreds of ports that require continuous protection, and there have been proposals to consolidate the federal agencies responsible for border security. This may offer some long-term benefits, but three challenges may hinder a successful implementation of security-enhancing initiatives at the nation's ports – standards, funding and collaboration.

The first element involves implementing standards that define what safeguards a facility should have in place. Under the USCG's direction, a set of standards is being developed for all US ports to use in conducting vulnerability assessments. However, many questions remain about whether the thousands of people who have grown accustomed to working in certain ways at these sites will agree to, and implement, the kinds of changes that a substantially different environment will require.

The second challenge relates to determining the amounts and sources of funding for the kinds of security improvements that are likely to be required to meet the standards. Florida's experience indicates that such measures are likely to be more expensive than many anticipate, and determining how to pay these costs and how the federal government should contribute will present a challenge.

The third challenge is ensuring that there is sufficient cooperation and coordination among the many stakeholders to make security measures work. Experience to date indicates that this coordination is more difficult than many anticipate, and that continued practice and testing will be key.

Analytical approach

One technology that may be employed as part of this process is video analytics. *IMPS* spoke to Eric Olson, VP marketing at PureTech Systems in Phoenix, Arizona, who explained the company's offering in this area.

'We are a geospatial, video analytics company. As opposed to traditional video analytics we include location data. In addition to seeing a person or vehicle in a video, we also know his exact location. This is our technology that we bring to critical infrastructures,' he said.

Geospatial or geo-referenced systems link data to real-world co-ordinates – latitude, longitude, speed, heading, altitude and time.

Olson detailed three primary areas of focus: the integration of sensors; the level of automation in the system; and the forensic demands placed on security officers. In particular, the ability to more efficiently filter video was seen as a major requirement for ports.

Additionally, map-based video management systems allow the operator to view a seaport and see where the sensors are located. They can then be dynamically controlled directly from the map, and any identified targets are updated in real time and tracked.

In the event of an intrusion, and preferable to looking at a hundred cameras and trying to determine where exactly the event is occurring, a map-based system will show a picture of a human and its exact location. As the intruder moves, the system will track their movement on the map, from one camera to another. This situational awareness helps the responder understand and handle a threat rapidly.

Among the challenges for seaports on the landside is affordability. Large perimeters and challenging terrain give rise to the problem of how to protect the facility and not break the budget. Video analytics can detect objects at very long distances, reducing the need for additional cameras and pole infrastructure.

'One of things we learned when working with seaports,' Olsen said, '[is that] there is an additional factor – manpower costs. Part of the issue of long perimeters is the need for more people to monitor the additional sensors often needed to cover these large perimeters. Reducing the number of sensors via longer detection distances helps to reduce not only infrastructure costs, but also recurring manpower costs.'

Given that a seaport is a very busy place, the system has to be sufficiently 'intelligent' to gauge what is normal and what is not, and what to activate the alarm for. Ports also require day and night-time operating capability. For this reason, many sites use high-resolution thermal cameras so the perimeter does not need to be lit.

Classification is another video analytics capability appreciated by ports. This is the ability to use video data and location information to understand that what is being observed is a person and not a vehicle, or vice versa. Classification can also determine the type of vehicles coming into a port and automatically manage security systems in dealing with specific situations.

'The map-based display is very important for seaports as it gives a quicker visual understanding of an intrusion, which is important for a long perimeter,' emphasised Olsen. 'With our system, you click on a region you want to view on the map and it will steer the camera to that exact location and adjust the zoom level to enable a quick assessment of the situation.'

Breaks from tradition

Given the continued heightened threat level in place in countries like the UK, the ability to effectively secure the perimeter of a diverse range of sites, as a first line of ▶

defence against potential terrorist attack, is undoubtedly a key concern for government agencies, police and security managers on the ground.

Whether the location in question is a transport hub or another element of national infrastructure, it is imperative that integrated and robust security measures are in place. The modus operandi of terrorists is constantly evolving, as is their willingness to consider extreme measures, even chemical and radiological attacks. The reality is that terrorists will look to exploit any perceived vulnerability to their advantage, so constant vigilance remains a necessity.

Optex Group has installed its laser scanner sensors at a range of critical infrastructures sites around the world. The technology allows the creation of a vertical virtual wall or horizontal panes. When employed for perimeter protection it can detect people either approaching or loitering around the fence to create a pre-warning zone, as well as alert security forces when someone actually enters the facility.

In addition, the company's fibre-optic perimeter intrusion systems (PIDS) can detect people cutting or drilling through the fence, climbing over or crawling underneath.

Optex's system – manufactured by sister company Fiber Sensys – has been designed for false alarm resistance, high capture rates and long service life. The sensing element is claimed to be intrinsically safe, immune to the effects of lightning strikes, or electrical, radar and radio interference and is also corrosion-free.

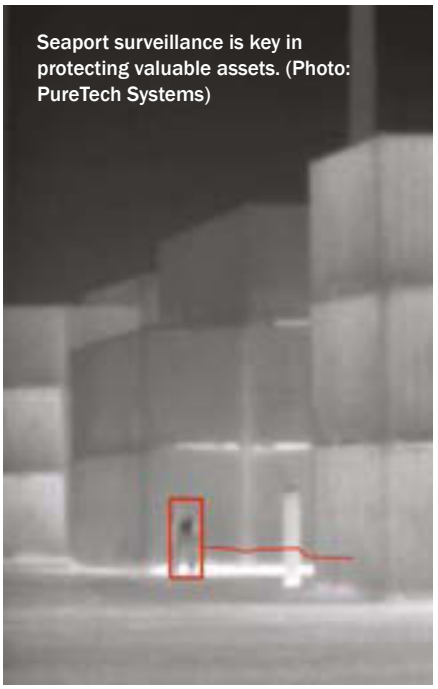
Command conclusion

However, as important as it is to sense a possible threat, the need to correctly categorise and analyse images brings much-needed efficiency to such operations.

'CCTV systems are useless if they cannot tell the difference between a burglar and the neighbourhood cat,' said Bill Flind, CEO of UK-based Ipsotek. 'Ipsotek was created to use video analytical techniques to identify potential problems at any time of the day, in good or bad weather.'

He said that the company's solutions are able to detect and highlight an object of interest's actual location in three dimensions: 'Where is that object in the real world? The simplest way to define this is to geo-tag that object by performing 3D modelling of the camera scene. Having achieved that, you can easily then find out how far and where that object is in reference to the camera.

'The system knows where the camera is and where it is pointing, so from there the GPS co-ordinates can be calculated for every object that is being tracked in the camera view.'



Seaport surveillance is key in protecting valuable assets. (Photo: PureTech Systems)

The deployment of 3D video analytics with GPS capability into this environment means that instead of just showing the operator a flat image with some bounding boxes, it is now possible to display the location of the object that triggered the alert onto a map or plan. This also graphically indicates the direction and speed of travel of the object and, more importantly, its distance from sensitive assets.

Flind further described the effectiveness of this technology in that it automatically controls the cameras to zoom on and track the target to further assist operators and provide more control of an unfolding incident.

It is clear from the technologies being developed that perimeter protection is as much about sensing, analysing and categorising threats as putting physical barriers in place to stop them.

Deterrence remains vital, so visible cameras and fences have a role to play. But should an incident involving non-state actors or other aggressors breaching a port's perimeter security occur then the system tasked with its defence must be able to play a role as the situation unfolds. ■

Networking can provide a greater integration of systems. (Photo: PureTech Systems)