**Patrik Anderson** explores the unique challenges of securing ports and cargo, and argues that IP-based surveillance systems offer multi-layered protection from terrorist threats

# CONTAINING

Shipping ports are a vital lifeline for supplying the world's population with the necessities of living. Between land, rail and sea, ports are the hubs of far-reaching networks that connect suppliers and consumers around the globe. As a result, operating these facilities safely and securely is a paramount concern for port operators, shipping authorities and the government agencies that police them.

Because of the typically diverse and sprawling nature of a shipping port, they can be extremely vulnerable sites. The geographical layout of the ports themselves makes protection and security of their perimeters difficult, especially considering their large size and varied surroundings. Since they are most often largely outdoors, weather conditions further complicate security. The high volume of trucks, trains and ships entering and exiting port facilities pose a threat to the port, as well as nearby geographical areas. The threats to security include intruders who wish to gain access to the facilities, as well as the items that may be passing though the ports themselves. The latter risk is increasing as shipping volumes continue to climb, putting pressure on logistics managers and inspectors alike who must find the most efficient ways to track, monitor and inspect goods.

In addition to the threats of theft, vandalism, smuggling of illegal or dangerous goods and unauthorised access, ports face an on-going threat of terrorist attack, which could have a devastating impact on the global economy if perpetrated in a busy port system. After 9/11, security requirements were enhanced in a number of locations that were considered to be a strategic target for terrorists, including ports. The International Ship and Port Facility Security (ISPS) Code was given a considerably stricter wording in order to prevent acts of terror.

Cargo containers represent the largest area of concern in terms of security and vulnerability. It is estimated that more than 12 million containers are currently in circulation, and securing, tracking and inspecting them all is a difficult task. A large container ship has the capacity to carry in excess of 10,000 containers, making inspection of each impossible without disrupting the shipment.

The security strategy for a large port facility must therefore consist of at least three types of security surveillance systems, ideally all integrated. First, the physical footprint and perimeter of the port itself must be monitored, including the vehicles used in the transport of good (ships, rail cars, trucks). Second, efficient and accurate inspection of containers is essential to monitor the goods passing through the port, as well as the condition of the containers. Third, access control is critical to ensuring that only authorised persons and vehicles can enter and leave the facility.

More and more ports are turning to the performance and effectiveness of high-resolution IP-based surveillance camera systems to assist them in their security procedures. In addition to high quality images, these cameras must operate in extreme weather conditions, challenging light scenarios (night and day), and also provide a range of advanced features such as thermal imaging. And they must be scalable to meet the dynamic needs of growing port facilities.

The scale alone of a modern port is challenging. For example, at the Port of Odense – one of the biggest ports in Denmark – an area equivalent to more than 100 football fields must be kept under surveillance. The port uses a network of 17 mobile and fixed pan-tilt-zoom (PTZ) cameras to provide the range and field of view needed; each camera can cover an area with a diameter of around 200 meters.

The cameras form the heart of the system, and high-resolution performance is critical, according to Jern Pedersen, Maritime Manager at the Port of Odense. "We can see considerably more than we expected with the high resolution cameras," he said. "We can now see when ships call at the terminals furthest out in the port and follow the loading and unloading without being on site."

Challenging conditions require additional features from cameras. For example, thermal imaging systems enhance the system by providing high-quality imagery in the dark or night or challenging environmental conditions like fog, haze, or rain.

An effective port security system must notify security personnel when an intrusion occurs. The system used at Odense includes an intelligent application that detects anyone entering the area and triggers an alarm. Intruders can be detected and identified even if they are far from the camera, and it is also possible to set the camera to follow people and vehicles automatically. When the object is out of range, the next camera takes over. Because of the high quality images produced by the cameras, perpetrators can often be quickly identified and prosecuted.

Such systems also saves money and time through their remote control capability, which means guards can evaluate a situation and the degree of response required without needing to visit the scene. If a patrol needs to be sent out, they can use a mobile connection to see where the intruders are going. If it is assessed that the police need to be called, the police can also be given access to the camera footage remotely.

# THE THREAT

A major challenge of port operators is the inspection of containers. Again, volume and scale are daunting. At the Virginia International Terminals, for example, around 700 cargo containers flow to and from the rail yards at its facility in Norfolk, Virginia each day.

To deal with the inspection challenge at that facility, rail volumes were consolidated onto six tracks in the centre of the terminal. To monitor this area, 32 networked dome cameras were mounted on 100-foot high poles surround the central yard. Because the rail yard already had an IP infrastructure in place, the cameras could be attached to the existing fibre network like any network peripheral.

With pan/tilt capabilities and 35x optical zoom, the networked cameras give inspectors vantage points from which to remotely examine containers in an area that stretches a length of more than six football fields. Inspectors sit at their workstations and use a joystick to instantaneously manipulate the cameras to zoom in on a container's number, the slot number of the rail track and the rail car number from which it originated. A video wall of high definition monitors display container detail that inspectors then input into the database.

In addition to tracking information, cameras can be used to evaluate a container's condition. Cameras can be mounted on the reach stackers that are used to load and unload containers; these can be controlled through wireless networks to scan the container and transmit images. Inspectors reviewing the video images decide whether to send the container on its way, flag it for repair or reload it contents into another container. The images also serve as proof that any damage occurred before or after the terminal handled the container.

"It's a lot faster for the network cameras to take pictures of the containers than for inspectors to walk all that distance on foot. Plus you don't run the risk of an inspector being hit by one of those massive cranes or stackers," said David Linquist of Port Solution Integrators, which implemented the security installation at the Norfolk facility.

Other emerging areas that port operators are looking

***The geographical layout and weather conditions of ports makes them extremely difficult to secure effectively***


©Getty Images

# CONTAINING THE THREAT

to in order to assist with container inspection include optical character recognition (OCT) to automatically digitise container, track and rail numbers. This will enable inspectors to replace manual input of tracking data with a single keystroke. In addition, analytic software to highlight container anomalies will help inspectors respond more quickly to problems that need their intervention.

By using an IP-based security systems, port security officials can easily add in sophisticated access control systems. With open IP solutions, the access control units can use existing network infrastructures. Power locks, readers and other entry equipment are now available with Power over Ethernet, which means one single cable provides both the data connection and electrical power; cabling is therefore hugely simplified. With an open application programming interface (API) and configurable I/O ports, these systems use standard Internet and connection protocols and can be easily integrated with other IP-based devices – from surveillance cameras to intrusion detection. This greatly improves the ability to monitor access to a port which has a typically challenging perimeter and variety of access points.

With an IP-based system, every access control unit represents a smart independent device that is installed by each entry point. The units include integrated software for basic access management, as well as more sophisticated software that integrates and communicates with other systems in the network. Such a solution is not only flexible in terms of integrating it with other connected devices, it is also freely scalable – a critical consideration for a growing port facility. Access control systems built on these units can be extended to any size, from small installations to advanced installations that meet the needs of large facilities.

A huge range of functions can easily programmed into the administration software, including managing cardholders' permissions and user groups, locking doors and gates remotely, and tracking events and sending out automated SMS notifications in case of an irregularity. These can then be controlled from any authorised computer or handheld device that is connected to the network wirelessly.

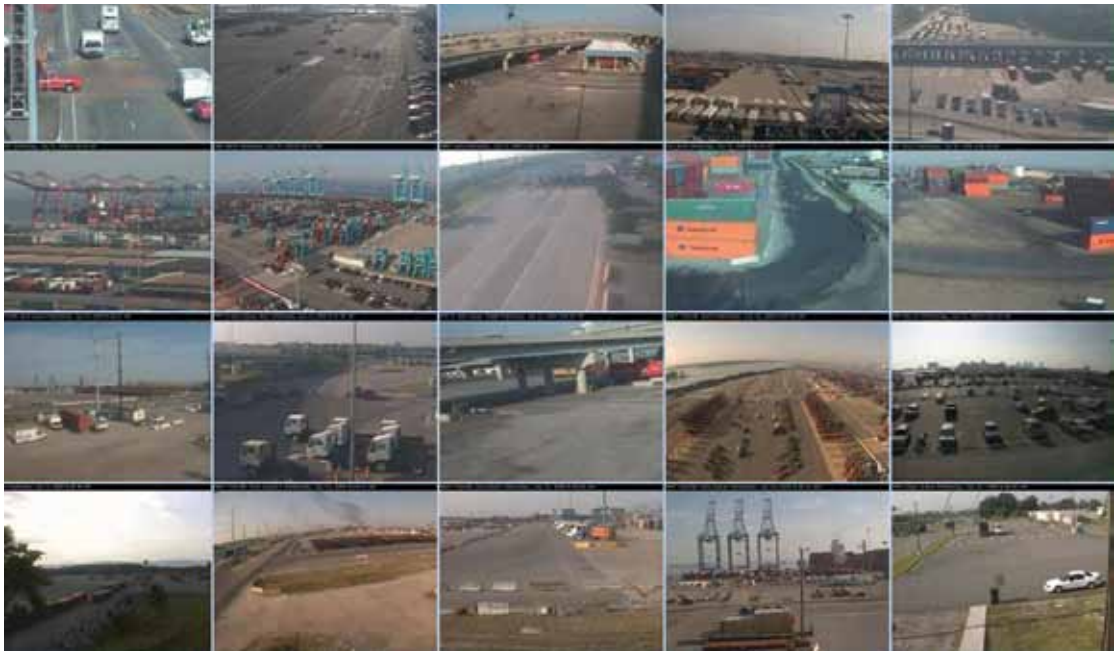
The shared information such as system data, user credentials and configuration settings are all automatically synced between all smart units in the system. This also makes adding new devices and extending the installation extremely simple, as existing cardholders and system data can be imported onto the new controllers.

As an open platform for integration, IP-based access control units with an open API can run several types of software in parallel. Access control software with flexible functionality is the obvious example. Video management software allows the additional, easy integration of the door unit with network video cameras for enhanced usability and security. With video management software, access control events can automatically trigger the recording of video, for example when access to a door has been denied, an invalid card is being used, or an individual tries to force a door open.

Over and above this, a platform for physical security integration management would enable the management of a whole range of different security systems such as video, access, intrusion and motion detection, all through one common user interface.

A shipping port is a business and it must remain competitive in order to operate. In addition to helping meet mandated ISPS requirements, a modern security system can also reduce operating costs for a port facility and improve its overall efficiency. Since ports are funded by the dues and fees paid by ships, railroads and shipping companies, cost is an important factor; if it becomes too expensive to use the port, goods will be transported elsewhere. And carriers need to know that their goods can pass through the port safely and efficiently, and that they are being transported correctly. Therefore a comprehensive and well-designed security system is a valuable investment for any type of port.

**Patrik Anderson** joined Axis in 1997, and is focused on building the company's offering and presence in the transportation sector on a global basis. The transportation sector includes public transport, aviation, traffic, maritime and cargo. Mr. Anderson has a great deal of experience in business development in many industry sectors, as well as long leadership in product management and project management.



*IP-based surveillance systems, coupled with advanced software tools, can easily be integrated into existing surveillance infrastructure*