All necessary measures

Major seaports are large, vulnerable targets confronted by an increasingly complex range of high- and low-level threats. **Claire Apthorp** looks at the balancing act required to stay safe while remaining open for business.

The past two decades have seen a dramatic shift in the spectrum of threats port areas have to deal with to remain secure. In addition to keeping vessels, passengers, employees and cargo within the facility safe from accidents, the authorities must have the means to monitor and protect against the persistent threats of terrorism, smuggling and illegal immigration.

The motivation is high – to fail to have adequate security systems in place that provide a safe port environment while allowing business to continue unhampered poses significant risks to the viability of the facility itself, the companies that rely on its services, and the economic health and security of the city it is located within.

RISING TIDE

One of the greatest threats to port security is the increasing incidence of organised crime, including cargo theft, terrorism, piracy and illegal immigration.

'We are now all very conscious of the risk posed by these threats that are both real and potentially fatal, and we are now being forced to take all possible measures to protect our ports from attack,' John Dalby, chairman of Marine Risk Management, said at this year's International Port Security conference in London in June. 'The shipping industry is responsible for the carriage of 90% of the world's commodities and that makes it a very tempting target – both afloat in our ships and ashore in our ports.

'Additionally, our ports represent a particularly vulnerable target because they are approachable from both the land and the sea, and from within ships and cargoes that arrive and are handled there. The challenge we face now and in the future is to ensure that our ports and hinterland remain safe and our economies free from disruption by those who seek to harm international trade.'

A focus on changing maritime safety requirements at the IMO began in 1985 with the hijacking of the cruise liner *Achille Lauro* by terrorists. In response, the 1988 Suppression of Unlawful Acts treaties aimed to stop the seizure of ships and offshore platforms, committing acts of violence against persons on board or causing destruction or damage to ship, platform, cargo or maritime navigational facilities, or the placement of devices or substances to destroy or damage ships or platforms.

Since then, the bombing of the USS *Cole*, the explosions on the *Limburg*, *SuperFerry 14*, and *M Star* vessels and the World Trade Center attacks in 2001, have driven forward regulations for measures to enhance maritime security in the SOLAS (Safety of Life at Sea) Convention's chapter XI-2 and the International Ship and Port Facility Security (ISPS) Code.

'The key difference that has emerged is that in the *Achille Lauro* days we were concerned about

Seaport containers are removed from a ship for further inspection. (Photo: US Customs and Border Protection)

Many ports remain reliant on CCTV footage to control access to restricted areas as part of their security system. (Photo: Port of Santos)

ships being the victims of terrorist attack, but that changed with 9/11 because ships became weapons in the same way that aircraft were used as weapons against the World Trade Center,' said Andrew Winbow, the IMO's director of maritime safety and assistant secretary-general. 'The SOLAS convention is the tool to raise the bar of security for ships and ports, and contains functional requirements for ships and port facilities to introduce systems to detect and deter acts which threaten security.'

ASSESSING REQUIREMENTS

The security required for port areas is based on a risk assessment or sea survey that determines on what basis measures should be put in place, how they will be managed, and how the chosen solution can be adjusted in line with changing threat levels.

'The idea is to look at your port, identify the areas that are at risk, look at what is happening and make a suitable plan based on the risk that you understand to be the case,' Winbow said. 'For ports, this requires looking at things from a security perspective, which might be very different from a perspective of efficiency.'

Since 9/11, ports must also be capable of protecting themselves against vessels, which requires threat management to be conducted on all ships within the port area. This includes the use of AIS to identify what vessels are in or approaching the port, vessel traffic management systems (VTMS) to monitor movement within the port, and long-range tracking systems for traffic further afield. State control provisions also give port authorities the opportunity to inspect ships of any nationality in their facility, and are based on all vessels carrying an international security certificate.

TECHNOLOGY FOCUS

The security infrastructure designed to mitigate risks to port areas is increasingly sophisticated, and many responsible authorities around the world are working to upgrade their systems to meet the evolving challenges facing the sector. From fencing and gates to CCTV-based surveillance and high-technology radar, the infrastructure must control access to the port while allowing efficiencies to be maintained as much as possible. It must also be scalable and able to deal with different threat levels, as determined by government organisations.

However, the case for safety in port areas is often at odds with economic factors, which can hamper the acquisition of new security solutions.

'The number one reason for ports is to move cargo through to make money, and the second is to attract, maintain and service the shipping companies so they can make money – the third goal might be safety if it doesn't interfere with making money,' Capt Donald Farrell of the Los Angeles Port Police said.

'[In other organisations] a good idea for public safety stands on its own merits, but when you are operating in a port environment every good idea is held up against the first two goals, so sometimes convincing the managers of ports that a security system or change in procedures and protocols [is needed] will be met with opposition.'

As a result, any new measure must allow business to continue, unimpeded by lengthy and complicated procedures. It must also be cost-effective and reduce operator workload, and be easily integrated into a central management system that can monitor and regulate data to create situation awareness of the port while minimising false alarms.

CAUGHT ON CAMERA

Ports are continually reassessing how to meet their evolving security requirements. In 2009, the Port of Dover made the decision to outsource all of its manned security services

One of the biggest challenges for port authorities is to manage and control the significant numbers of vehicles moving through the port each day. (Photos: Port of Santos)

The Port of Santos is the largest port in Latin America, with a total area of 7.7 million square metres.

to a third-party contractor as part of a programme to improve its ability to comply with legislation, deliver a secure environment and continue to run an efficient business.

As the busiest, most intensely trafficked roll-on roll-off (RORO) ferry port in Europe, Dover handles £90 billion ($150 billion) worth of cargo every year. Over 120 ferry arrivals/departures at the port carry up to 9,000 trucks, 16,000 cars, 350 coaches and at peak times up to 60,000 passengers per day. Additionally, the port handles around 155 liners per year with 250,000 cruise passengers (each carrying 2.4 suitcases), plus 150 reefer vessels and 5,000 yacht visitors, while its marina hosts 350 berth holders.

According to Paul Brown, Dover's general manager of port operations and harbour master, maintaining the security of such a facility, while keeping the site running and the traffic fluent, is a hugely complex task that involves people, equipment and technology.

'Ensuring the integrity of the security area involves controlling access to the port area, controlling and recording whomever leaves and enters, and controlling who parks what where and for how long,' he said. 'Under obligations to the ISPS Code we have to ensure that a defined percentage of our cargo – trucks, coaches, people, containers – is searched and screened for items which pose a security threat; and under this sits the UK Port Security Regulations 2009 which formally require me to deliver a specific security regime.'

> 'Of course, CCTV is not without its problems... particularly when operating in high-salt and wind environments.'

Under the security outsourcing project, G4S tailored a solution to manage the whole dockside service. Under its contract, the company provides security staff trained to ISPS levels and competent in the use of x-ray and search equipment, as well as baggage, cargo and passenger handling and assistance.

The port also rolled out the use of new explosives trace testing technology in 2014, which has tripled search rates and contributed to increased safety.

For surveillance within the port area, Dover has over 110 static CCTV cameras monitoring activity 24 hours a day, with a limited recording capability. As well as providing the mainstay of the port's security plan – chiefly as a means of maintaining the integrity of restricted areas – CCTV also has wider utility for operations, providing a real-time ability to monitor traffic flows and the formation of queues both inside and outside the port.

STARING EYES

Dover also uses the Highways Agency's cameras on the motorway network to gain intelligence of traffic heading to the port, and various arms of the police services use port CCTV cameras for border control purposes.

'Of course, CCTV is not without its problems, particularly when operating high-technology electronic equipment in the high-salt, moisture and wind environment of southeast Kent, where fog and spray can [often] severely limit vision,' Brown said. 'Additionally, modern cameras are fairly robust but salt corrodes just about everything, and keeping them secure, safe and – most importantly – pointed at what you want them to be pointed at poses a challenge.

'It can happen that the one area you do need to look at after a security event is the one area where there was a coverage blank, and if you do have coverage it can happen that the CCTV camera either didn't work or has just overwritten the bit of data of relevance. Data storage is often

an uninteresting and dull backwater, right up until the moment you want to see that data.'

In order to address these problems, the Port of Dover is in the midst of a comprehensive review of its CCTV requirements. One solution involves the purchase of a central data store, where the information provided by cameras can be processed in one location, utilising a digital network that will require fibre optics, and agile computing power.

The final aspect of security at the port concerns access control. Dover utilises equipment that monitors and records access to restricted and controlled areas of the facility, administering over 6,000 permanent pass holders and the 800+ temporary passes that are issued every week.

EVOLUTIONARY PROCESS

Brown accepts that the security of a facility such as the Port of Dover is a continually evolving process, and that 'staying ahead of the game' is an ever-present challenge.

'Have we had our 9/11 yet? I don't think we have,' he said. 'We are still to have our terrorism spectacular, and we must ask ourselves this question because the marine back door is still open, and we must do what we can to protect ourselves in the future – we cannot relax, the problem isn't going to go away, and the answer will include more training and more awareness of the potential threats.'

Brown considers the marauding terrorist firearms attack – as seen in Mumbai, Nairobi and to a limited extent Stockholm – as the highest threat. In illustration of how seriously this is taken, the port will be closed for four hours in September for a multi-agency exercise involving resources across Kent to rehearse reactions to such an event. The exercise will be the first of its kind in a UK port.

'One thing is for sure – if I am asking these questions about the marine threat, there are plenty of other governments asking the same ones, and I'd be very surprised if we cannot expect more legislation to attempt to force port operators to adopt ever more intrusive and expensive security measures,' he said. 'We in the marine industry are the poor relation of the aviation industry when it comes to security, and we still face the hard task of educating the uninitiated.

'My passengers arrive in their cars and have a very real expectation to roll on/roll off without interference. If I get my security measures wrong, the delays manifest themselves on the national road network, and with the entire philosophy for the RORO industry for the last 40 years having been built around the fast and fluid movement of passengers and freight, anything that interrupts that is bad for business.'

KEEPING TRACK

As the largest port in Latin America, the second largest in the Southern Hemisphere and with a hinterland covering 55% of Brazil's GDP, the Port of Santos is an immense facility. It has a total area of 7.7 million square metres, a 13km-long pier, 53 public and 11 private berths, a storage capacity of approximately 700,000m^3 for liquid bulk, warehouses for packing more than 2.5 million tonnes of solid bulk cargoes, and a patio area of over 981,000m^2.

A significant challenge is to provide security with large numbers of vehicles moving through the port every day. Santos uses an electronic registration system called Common Database Accreditation (BDCC) that compiles lists of companies, people and vehicles approved by customs to manage entry authorisation. Every truck wishing to enter the port must be registered and fitted with an RFID tag, which aims to identify vehicles automatically, using technology similar to 'no-stop' toll booths. Similarly, every driver must be registered to gain access, with the database providing for the use of biometrics.

The port also has plans to roll out optical character recognition technology to monitor the number of containers travelling on registered trucks as they pass through points of entry, as well as the use of electronic seals on containers to tamper-proof the contents, and scales at the gates to control entry and exit loads. As well as contributing to security, these solutions have a significant impact on automating logistics processes.

The Port of Los Angeles (POLA) – as the leading container port in the US and a critical hub in the international supply chain – has also received an upgraded access control, CCTV and video content analysis system, provided by G4S Technology. The company designed, built and integrated additional cameras into the port's current security system. These were strategically placed, providing a higher level of video protection to key areas within the complex. In addition to expanding the video analytics system, G4S Technology added sensors, access control and system monitoring capabilities.

SURVEILLANCE GAP

While many ports are deploying sophisticated surveillance capabilities to maintain the integrity of their perimeters, there remains a surveillance gap which Sonardyne International aims to meet with its Sentinel Intruder Detection Sonar (IDS) system.

The Port of Dover is one of the busiest RORO ferry ports in Europe, handling some £90 billion worth of cargo every year. (Photo: Wikimedia Commons)

'From fences to CCTV, EO cameras, thermal imagers to long-range radars connected to AIS and short-range radars looking for small vessels, users have the ability to bring a great deal of information together to meet their surveillance capabilities,' Sonardyne business manager Nick Swift said. 'But we see that there remains quite a vulnerability in addressing the underwater threat, so while they have very good awareness at the surface, there is very little that can actually give an underwater situational awareness to warn of threats coming that you can't see.'

Sentinel IDS can be configured to provide long-range, wide-area detection, tracking and classification of underwater threats, using software that combines data from multiple sonar sources to produce a single picture of the environment.

The sonar technology can be deployed in a vessel or harbour environment to provide 360° of protection. Sentinel IDS can operate as a standalone portable solution or be configured with multiple, networked sonar heads so that very wide areas, such as large ports and entire waterfront locations, can be protected. It can be integrated with an external command and control (C2) system, and is operational with customers in the US, Europe, Africa, the Middle East and Asia.

GEOGRAPHIC UNDERSTANDING

A unique aspect of port facilities is that they do not exist in isolation from their surroundings. They present a significant vulnerability to the wider area, given that the defence of ports is hindered by the difficulty of separating friend from foe in the cluttered sea environment, and the relatively short reaction times when a threat is identified. In the event of an emergency being declared, either inside or outside the port area, there must be systems in place that can draw together situation awareness of the entire site to aid emergency responders in decision-making.

Geographic information systems (GIS) are increasingly being deployed to provide this capability. This technology allows users to view, understand, visualise and interpret data from multiple sources – CCTV, radar, VTMS, thermal imagers and AIS receivers – into a single operating picture of the facility. Rendering the data visually reveals relationships and patterns to inform decision-making; essentially showing what has happened, what is happening and what will happen in a geographic space.

> 'There remains quite a vulnerability in addressing the underwater threat.'

In a port environment, GIS can integrate information from all aspects of operations, helping to manage environmental compliance and emergency response planning, provide a common operational picture of facilities, including security monitoring, and improve operations through more precise coordination.

Such a system has been rolled out at POLA by NorthSouth GIS using an Esri-based enterprise GIS that addresses operational, security and emergency management issues, with data and ready-made maps served directly from an Esri ArcGIS server – a platform for designing and managing solutions through the application of geographic knowledge – to other software and systems including situation management. This provides an integrated display of static GIS data and dynamic data including vessels, traffic, weather and blue force tracking for port police, and delivers and integrates geospatial information via a port-wide intranet GIS web map viewer known as geoPOLA.

INTEGRATING CAPABILITY

The ultimate goal for many ports is a single C2 solution that integrates all the different security measures employed in an area to provide an overarching situation awareness picture for operators.

In June, a consortium comprised of Ericsson, INDJAZ, Korea Trading & Industries and Kongsberg Norcontrol IT was selected to deliver the Algerian national Vessel Traffic Management and Information System (VTIMS). This aims to improve the safety and security of maritime traffic to, from and within Algerian ports by tracking vessels and facilitating movements. It will also provide early warnings of potential collisions and groundings, and will include a solution provided by Ericsson that provides video surveillance with access control, intrusion detection, perimeter protection, passenger and goods control.

Saab's SAFE security management system offers a similar capability, providing a flexible, scalable and robust solution for infrastructure protection and emergency response. The system's C2 provides security centres, administrators and field forces with a common situational picture and tools to deal with threats or incidents, as well as providing statistics and analysis data, GIS and video management.

The self-monitoring system gives users a resource to gather, validate, classify and prioritise all security information in one place, with no technology dependencies on specific products and vendors, reducing costs by integrating multiple disparate products.

Such systems offer high-technology capabilities for ports seeking integrated all-in-one solutions, and with many facilities still relying on disparate security systems operating in isolation, they offer a significant increase in coverage. As port facilities continue to address evolving security requirements, the deployment of these solutions is likely to increase, resulting in safer, more efficient environments than ever before. **IMPS**