Unified security to protect critical port infrastructure

David Lenot, *Director Transportation EMEA, Genetec*

As the largest container port in the world, the Port of Shanghai spans 3,619km^2 and handles over 744 million tonnes of cargo annually. If its size alone does not make it difficult to secure, the thousands of people from ships, trucks and cargo companies coming and going daily and the massive waterways leading into docks contribute to the security challenges.

Regardless of size or the types of vessels coming into harbour, ports are challenging security environments. Port security departments must rely on technology such as IP video management systems (VMS) and ultra-megapixel cameras with long-range zoom capabilities; these help keep an eye on incoming vessels, watch people moving through the terminals, and detect any suspicious activities or possible threats before they wreak havoc on operations or people's safety.

However, more international ports are also looking for better ways to improve effectiveness in their operations and response. They realise that they can achieve this by combining IP VMS with other security technologies such as access control, intercom, license plate recognition, perimeter intrusion detection, radar and vessel detection.

While most might consider security the main objective to implement such technologies, including protecting people and assets, ports are leveraging their security investments to also improve operations. Mimicking the likes of international airports such as Amsterdam Schiphol that uses an advanced video surveillance system to dispatch more customs agents when they notice above-average passenger congestion or to adjust baggage carousel designations in case planes are delayed, ports are increasingly seeing the benefits of technology beyond security.

For ports, operational benefits might include keeping an audit trail of vessels and trucks coming to pick up and drop-off cargo, dispatching more customs officers to greet incoming passenger ships, or using video evidence to dispute liability claims or damaged property.

But how are ports implementing these technologies? And what system features help to ensure a successful and cost-efficient installation of multiple systems?

Five systems to integrate with video surveillance

Access control integration – Video surveillance and access control are some of the most common integrations in any security application. In a port environment, access control readers can be deployed at the main entrances, restricted areas and port facilities. Since so much technology has evolved in access control, ports are offered many interesting options such as all-in-one locks that provide a more simplified installation, wireless locks which are ideal for hard-to-reach locations, and biometric readers or handheld readers that suit more critical areas.

For instance, the Manchester Terminal, a private marine terminal in Houston, Texas, implemented a government-run security programme called TWIC (Transportation Worker Identification Credential) which provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities. They accomplished this by adding TWIC-compliant handheld readers with identification and biometric matching software which allowed the security guards to process credentials and inspect trucks. The handhelds also allowed them to go to the ship docks and check the credentials of people coming-off ships and spot-check compliance around the facility.

Licence plate recognition integration – In similar respects, synching license plate recognition (LPR) technology with access control and video surveillance, allows for monitored and gated vehicle control at the perimeter entry or at restricted personnel-only zones around the port. Port authorities can deploy fixed LPR cameras at entryways which scan vehicle licence plates and, based on a permitted list, either denie or allow entry.

These cameras can also be used to collect an audit trail of trucks coming in and out for pick-ups and deliveries. In a mobile installation, LPR cameras can be placed on a vehicle; port authorities can drive around loading docks to capture time-stamped license-plate reads and pictures of the trucks. The information can also be tied to GPS coordinates, so in the event of any liability issues, or missing goods, information concerning the truck, the time of pick-up and its location are available to dispute any false word-of-mouth claims.

Perimeter intrusion detection integration – Much like airports, ports have huge landside perimeters to protect. Many international ports rely on technologies such as microwave sensors, fence detection sensors, buried cable detection sensors and even trip-wire analytics.

To complement perimeter detection,

Screen-grab of Genetec's Security Center software for the physical security and public safety industry

Left: Port Freeport; Right: Aerial view of Port Freeport, Texas, US.

placing high-resolution cameras that capture clear, long-range imagery is helpful. With strategic configuration, the first line of perimeter detection at the fence will prompt alerts that trigger cameras to automatically pan-tilt-zoom into the target area for visual identification. Video surveillance is then sent directly to the security monitoring centre, or even as a mobile alert to the security director's smart phone, for immediate verification and response.

Vessel-radar integration – Massive waterways and channels leading into ports must remain open to boat traffic and cargo vessels. Because of the size and area of these bodies of water, they are particularly difficult to secure and are susceptible to vulnerabilities. Ports such as the Port of Freeport on the Gulf Coast in Texas, US, are using vessel-radar systems to identify small craft or other unsuspecting anomalies, and automate pan-tilt-zoom (PTZ) functions on video surveillance cameras to have instant video verification.

Key criteria for successful port security

While there are many system functionalities that allow ports to tie in and efficiently manage all these systems, three key security platform characteristics will ensure their investments remain worthwhile for many years to come: 1) an open architecture; 2) unification; and 3) centralised and shared access to common devices and systems through Federation – which gives ports the ability to easily share video feeds or access specific cameras located on common waterways.

For one, choosing an open architecture platform is one of the most important tactics in ensuring a future-proof investment. Most ports already have significant investments in video surveillance technologies and are not prepared to undergo a complete 'rip and replace'. This is why ports benefit from open-architecture video systems that allow them to incorporate their existing analogue or IP cameras and easily upgrade devices over time.

Open-architecture systems also avoid locking ports into specific vendors or devices, giving them complete freedom to choose the devices that best suit their applications or budgets. An open architecture also facilitates third-party integrations with other security systems; but this is where unification comes into play. By unifying their security platform to act as a central point of information and control for all security and intrusion-related events, ports can achieve greater 'correlative' situational awareness to monitor open, widespread grounds or waterways.

A unified system is specifically engineered to manage multiple security systems in one platform from a single vendor, thereby providing both a unified interface and back-end server infrastructure that offers fluid and fault-free version upgrades. Unification also allows operators to streamline workflows within a single platform that synchs all security system management capabilities, such as monitoring, reporting, alarm management, configuration, authentication, permissions and more. All of this leads to less training, more efficient day-to-day operations, and easier investigations. When possible, considering unification over integration is always an easier, more cost-effective method to merging multiple systems.

But ports alone do not necessarily run standalone. There are typically many stakeholders that are involved in securing these critical infrastructures such as customs, coast guards, surrounding port facilities or private organisations. In a multi-stakeholder environment, it becomes important to share information. In the event of an emergency, Federation can be utilised; it also allows these multiple agencies to share the costs of equipment, offering more video coverage or data for far less cost than procuring the systems or hardware alone.

Sailing into a unified strategy

Ultimately, many new technologies are available to ports for not only securing their perimeters and waterways but also to boost operational efficiencies and streamline processes. Whether that means combining existing technologies or adding new systems such as access control, license plate recognition, perimeter intrusion detection and vessel-radar systems, opting for an open-architecture and unified platform with federation capabilities is the best way to ensure long-term benefits and cost savings.

About the author

David Lenot recently joined Genetec as director of transportation in the EMEA region where he is responsible for developing tailored solutions in coordination with transport customers to help them increase security and reduce operational costs for complex projects. Lenot joined Genetec from Bosch Security Systems where he was business development manager - IP Sales - EMEA. With over a decade's industry experience globally, he has helped numerous airports, subway systems, and railway operators implement complex IP-based security infrastructures.

About the organisation

Genetec develops open-platform software, hardware and cloud-based services for the physical security and public safety industry. Its flagship product, Security Center, unifies IP-based video surveillance, access control and license plate recognition (LPR) into one platform. A global innovator since 1997, Genetec is headquartered in Montreal, Canada, and serves enterprise and government organisations via an integrated network of resellers, integrators and consultants in over 80 countries. Genetec was founded on the principle of innovation, and remains at the forefront of emerging technologies that unify physical security systems.

Enquiries

Genetec UK
400 Thames Valley Park
Reading, Berkshire, RG6 1PT, UK
Tel: +44 (0)1189 653 605
Web: www.genetec.com