Companies and agencies involved in maritime trade must implement an unprecedented range of security and safety measures. For many port and vessel operators, the process of installing security systems that comply with the new requirements will continue to be a daunting task for the foreseeable future.

Clearly, the maritime industry is one of the most powerful drivers of international commerce and economic vitality in the world. The statistics are astounding:

- The worldwide fleet of marine containers, a transportation cargo unit that can hold up to 500 computer monitors, is nearly 11 million
- The European Union, which is the main trading partner for two thirds of the world, exports and imports over EUR 1,000 billion a year
- The global ocean-liner shipping industry owns approximately $155 billion in vessels, containers, marine terminals and other direct operating assets in service around the world
- Almost 16 million Americans work in port-related jobs, producing $210 billion in federal, state and local taxes annually

Security in the maritime industry has seen major changes since 9-11. Two months after 9-11, the International Maritime Organization (IMO) agreed to develop "new measures" for enhancing the security and safety of ships and ports. By December 2002, the IMO had defined and ratified its comprehensive approach as the International Code for the Security of Ships and of Port Facilities (ISPS).

The ISPS code's primary objectives are to establish a framework for the IMO's "contracting" governments to cooperate in taking preventive measures against security and safety threats that could affect the maritime industry. The ISPS code also outlines a methodology for ports and vessel operators to assess their particular levels of security risk and describes mandates they must fulfill to comply with the code. As required by the ISPS, contracting IMO governments have begun to pass legislation that mirrors the requirements and deadlines for compliance outlined by the new code.
In the U.S., the Coast Guard, working with government agencies such as the Department of Homeland Security, is responsible for monitoring compliance at ports and vessels.

**What the ISPS means for ports and vessels**

ISPS requires companies and agencies involved in maritime trade to implement an unprecedented range of security and safety measures. For many port and vessel operators, the process of installing security systems that comply with the new requirements will continue to be a daunting task for the foreseeable future. Some of the concerns that industry now faces include:

- **The high costs of compliance.** Although contracting governments are obligated to help fund the costs of added security in their country, the financial burden of installing new equipment, training people and managing new security systems ultimately resides with port and vessel operators. For many operators, the question of how they will fund the high costs of compliance — an ongoing operational cost — is the single biggest concern they have with the legal requirements.

- **Best efforts may not be good enough.** Never before have port and vessel operators been required to comprehensively assess their security needs and implement a plan for reliably reducing security and safety risks. For these operators, the process of outlining and implementing an effective plan that both meets regulatory requirements and stays within the limits of their operational cost structure may be a challenge they are unable to fulfill, despite their best efforts.

- **Minimal compliance (or none at all).** It is likely that many ports and vessels will try their luck, waiting to see what actions enforcement agencies take with others who are noncompliant before deciding to make a full commitment to security and safety. While some may slip through the cracks for a time, most who fail to comply face stiff fines and lost business opportunities from boycotts by other ships and ports.

**Conventional security and safety systems don’t meet the need**

The face of security and safety at ports has changed little during the last century. Almost all conventional security and safety systems available continue to be built around the same four fundamental characteristics that such systems have shared for decades.

Typically, these characteristics result in systems that are unreliable at promoting security and safety and are difficult and costly for the average business and government agency to implement and manage. These characteristics are:

- **Security specific.** Most conventional security and safety systems work in a vacuum, divorced from other business processes. These conventional systems in no way help to enhance business productivity or otherwise assist managers in running a stronger, more efficient business.

- **Paper based.** Conventional security systems typically rely on paper forms of identification (I.D.), such as drivers' licenses and social security cards, to verify the identity of individuals looking to access secure areas of a facility. Paper forms of I.D. — which colleagues can share and criminals can steal or forge — are inherently unreliable when used to verify identity. The process of screening paper-based I.D. typically requires recording data, such as a driver's license or Social Security number, by writing it down or making photo copies — a time consuming process that risks infringing on privacy rights.

Contrast this with the 225 biometric hand readers that help manage over 75,000 workers at Portos de Santos in Brazil, eliminating paper and its mistakes, costs and low security.

- **People driven.** In order to screen paper forms of I.D. and track the movement of individuals throughout a facility, an organization needs to employ security personnel. Security personnel are often difficult to train, costly to hire, and undependable.
Creating shipshape security at ports

- **Point oriented.** Conventional security systems are designed to secure specific points, or areas of concern, at a facility. Specific points include cargo, entrances to a vessel, and equipment. Because conventional approaches focus on specific points, one facility may have several disparate security systems serviced by different vendors.

For instance, a CCTV system installed by one vendor for monitoring cargo may work independently of an access-control system installed by another vendor for granting access to truckers who transport cargo. A facility that relies on point-based solutions is invariably inefficient, poorly accommodates change and growth in security needs, and can quickly become unmanageable.

For certain applications, conventional security systems that use decentralized paper- and people-based systems may be a reasonably effective, if not optimal, approach for promoting reliable security and business efficiency. The manager of a small corporate office with a couple dozen employees and a handful of daily visitors, for instance, may determine that hiring a security guard or two to screen building badges suffices for the company’s security needs.

But in the complex world of maritime trade – where hundreds or even thousands of crew members, drivers, maintenance workers, administrators and longshoremen, employed by unaffiliated companies and agencies, work together to move goods in and out of a port – a system of security that relies on paper and people to track, manage and monitor vulnerable assets is both inefficient and undependable.

Instead, ports need to integrate the security and safety requirements for every element of, and activity that takes place, at a facility. These elements and activities may be categorized as people, openings, and assets.

For instance, a ship's "openings" include the engine control room, electrical control/equipment room, cargo storage area, bridge, and steering gear room.

A port’s “people” include longshoremen, crew, administrators, maintenance workers, and truck drivers. Assets for both a port and vessel may include the vessels themselves, equipment, vehicles, containers and cargo.

Ports need to connect people, openings and assets together through a connected information-technology infrastructure based on an expandable, open architecture. Data is generated through the power of electronics – access cards with electronic codes or biometric identifiers replacing paper forms of I.D. and significantly reducing the number of security personnel required for security screening.

By using an open architecture, a port’s system will easily accommodate the addition of new security applications (i.e., a remote-monitoring system) as modules to a shared database.

The result is a highly reliable system that coordinates remote-monitoring, access-control, time-and-attendance, CCTV surveillance and other technologies and processes designed to secure a facility’s assets. As a result, a typical port and vessel could enhance security and safety while also promoting efficiencies including:

- Track crew at ports of call. Under the ISPS, vessels must maintain and manage records showing the last five ports each member of its crew last visited. While a conventional security system using paper-based tracking systems would be hard pressed to fulfill this challenge, ports can leverage time-and-attendance with access-control technologies to generate easily the required information when required.

- Verify truckers. Likewise, ports need to screen truckers entering the port. By using biometric readers together with smart chip cards, the two largest ports in Europe, Rotterdam and Antwerp, have implemented a fast method of identifying drivers, avoiding costly transport delays while still ensuring the highest security. The hand geometry template has only 9 digits, leaving plenty of room on the smart card chip for additional information. At the entrance, the driver identifies himself by using the card together with the hand geometry reader. Scan information of his left hand is compared with the template information on the smart card. He repeats the process upon leaving.
Creating shipshape security at ports

Of special importance to transportation authorities, the biometrically-enhanced smart card system ensures that information cannot be manipulated or changed, the driver does not have to remember specific information such as a PIN code, the smart card cannot be transferred to other people, and mistakes as a result of typing in incorrect ID numbers are impossible

- Automated response to different security levels. If an emergency or threat to security arises, the port’s system should be able to quickly adopt different levels of access control, such as might be defined according to different MARSEC levels, for authorized and unauthorized individuals.

For instance, in an emergency that requires people to exit a vessel quickly, all major exits would open rapidly and automatically. For another threat, the system may close certain exits or allow only individuals with a specific authorization to pass through them.

- Minimize costs for damage claims. Although many port managers contend that their facilities are responsible for no more than one third of the total cost they pay annually to settle damage claims for damaged containers, they traditionally have not had a mechanism for proving their innocence. By facilitating the generation of easy-to-navigate reports and video clips that demonstrate at what time and location a particular container was harmed, the security system could help minimize costs associated from unfair claims.

- Identification Cards. The IMO has called upon contracting governments to issue "seafarer" identification cards that can be used to verify an individual’s identity to all personnel involved in the maritime transportation industry. In similar fashion, the U.S. is finalizing plans, albeit slowly, for a prototype phase of the Transportation Worker Identification Credential (TWIC), an electronic "smart card" that contains coded information, such as biometric identifiers and bar codes, for the 15 million transportation workers in the U.S. who need access to secure areas of airports, seaports and land border crossings.

The time to act is now

Conventional security and safety approaches are inadequate for the unique demands of a maritime environment. Port and vessel operators need to meet the challenges of complying with the ISPS and other enacted regulations. By creating an overall plan with an integrated, open architecture solution, port security systems can act as a foundation for accommodating a growing body of legislation and the industry's increasing reliance on technology. Such an approach will help operators save costs now and in the future while also ensuring that a port’s people, openings and assets are secure.

Learn more about port security

For more information about security at ports and ISPS requirements please contact a professional security consultant in your area by calling 888.758.9823 or fill out the Contact Us form on our website at allegion.com.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit allegion.com/us
Creating shipshape security at ports