

— **Integrated Security** —

***A New Approach for Ensuring the
Security and Safety of Ports and Vessels***

Published March 2004 by

**Maritime Solutions
Ingersoll-Rand Security and Safety
Ingersoll-Rand Company Limited**

Table of Contents

Introduction	3
About the ISPS.....	4
What the ISPS Means for Ports and Vessels.....	5
About Conventional Security and Safety Systems	5
Why Conventional Security Systems Won't Work for Maritime Applications.....	6
Our Philosophy, Our Solution.....	7
<i>Integrated Security</i> at Work in a Maritime Environment.....	10
Conclusion	11

*This paper was developed by **Maritime Solutions**, which operates as part of the \$1.6 billion **Security and Safety Sector** of global diversified-industrial firm **Ingersoll-Rand Company Limited** (NYSE: IR).*

Introduction

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.¹
- The European Union, which is the main trading partner for two thirds of the world, in 2001 exported EUR 981 billion and imported EUR 1,027 billion.²
- The global ocean-liner shipping industry owns approximately \$155 billion in vessels, containers, marine terminals and other direct operating assets now in service around the world.³
- Almost 16 million Americans work in port-related jobs, producing \$210 billion in federal, state and local taxes annually.⁴

Clearly, the maritime industry is one of the most powerful drivers of international commerce and economic vitality in the world today. Yet only recently, with the introduction of a new body of international regulations called the International Code for the Security of Ships and of Port Facilities (ISPS) have port and vessel companies and agencies been compelled to implement security and safety measures on a comprehensive, international scale.

Now, these companies and agencies are struggling to implement security and safety measures that are both reliable and cost effective. Many are finding that conventional approaches to security and safety possess too many limitations to fulfill both of these goals.

Fortunately, there is a better approach for securing ports and vessels – one that can enhance the effectiveness of technologies such as electronic-access control, time-and-attendance, and closed-circuit television (CCTV) monitoring while also improving business efficiencies. It can help operators of ports and vessels save money while protecting their most vital assets.

The leading provider of this innovative approach – which focuses on integrating security and safety throughout a facility – is Ingersoll-Rand, a \$10 billion diversified-industrial firm. Through its Interflex, Recognition Systems, Schlage, Geoffrey and several other market-leading businesses and brands, Ingersoll-Rand is one of the only companies in the world today whose security and safety solutions incorporate electro-mechanical, electronic, biometric, and integration technologies. Leveraging this broad range of capability, Ingersoll-Rand has devised a unique strategy that has enabled AT&T, Morgan Stanley, the U.S. Department of Defense and many other organizations to reduce costs and increase security. Through its Maritime Solutions group, Ingersoll-Rand now is bringing this pioneering strategy and expertise to ports and vessels around the globe.

¹ Source: World Shipping Council.

² Source: Commission of the European Communities.

³ Source: World Shipping Council.

⁴ Source: American Association of Port Authorities.

In this paper, we'll describe the elements of this innovative approach and explain why it will be able to help port and vessel operators reduce costs while protecting their employees and facilities. We will also describe:

- the new regulatory environment created by the ISPS and the impact it is having on port and vessel agencies and companies;
- why conventional security approaches are poorly suited for maritime applications; and
- how our methodology, which focuses on facility-wide security integration, will prove to be the only logical, cost-effective approach for companies and agencies that hope to fulfill their legal obligations as defined by the ISPS, U.S. Maritime Transportation Security Act, and other recently enacted legislation.

About the ISPS

Two months after the tragic events of September 11, 2001, the 162-member countries of the International Maritime Organization (IMO) unanimously agreed to develop “new measures” for enhancing the security and safety of ships and ports.⁵ 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. The 2002 U.S. Maritime Transportation Security Act, for instance, required the 300 coastal and interwaterway ports of the U.S., and the thousands of vessels that dock at them each year, to define their security plans by December 31, 2003.⁶ It also requires operators to implement security measures outlined in the Act by the same deadline provided under the ISPS: July 1, 2004.

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.

⁵ An industry organization formed by the United Nations in 1948 that facilitates cooperation between contracting countries with respect to maritime trade issues, such as security and pollution.

⁶ Source: Kiplinger 2003.

What the ISPS Means for Ports and Vessels

Few can deny that new security and safety measures are a necessary response to the rising threat of terrorism, drug and arms smuggling, and other criminal acts. Yet, the 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.**⁷ 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 — the single biggest concern they have with the new legal requirements.
- **Best efforts may not be not 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.
- **Increasing legislation.** The ISPS is divided into two sections: Section A, which describes currently mandated security measures, and Section B, which outlines additional steps ports and vessels may decide to take to enhance security and safety based on their individual level of risk. Some companies already have begun to implement elements of Section B both as a “best practice” and in anticipation that the measures it describes will eventually reflect required practice.⁸

About Conventional Security and Safety Systems

The face of security and safety has changed little during the last century. Although new state-of-the-art technologies such as CCTV monitoring and digital-video recording (DVR) are rapidly replacing or supplementing mechanical lock-based solutions, almost all conventional security and safety systems available today continue to be built around the same four fundamental characteristics that such systems have shared for decades. Typically, these characteristics

⁷ The congressional General Accounting Office estimates that implementing the new security requirements will cost \$7 billion during the next 10 years in the U.S.

⁸ Maersk, for example.

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 four 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.⁹ 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.
- **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.
- **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.

Why Conventional Security Systems Won't Work for Maritime Applications

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

⁹ According to an August 2001 report by the U.S. Justice Department's Bureau of Justice Statistics, with the exception of physical characteristics, identification methods (such as name, Social Security number or other account number) are "...inherently unreliable in the criminal justice context."

system of security that relies on paper and people to track, manage and monitor vulnerable assets is both inefficient and undependable.

In addition to being unable to accommodate the high volume of people that moves through a typical port, conventional approaches to security and safety possess other limitations that make them poorly suited for a maritime environment. These limitations include:

- **Too unreliable to secure many entrances at risk.** From a ship's cargo area to a port's entrance gate, ports and vessels possess dozens of vulnerable areas through which unauthorized personnel can conceivably gain access. Protecting these entrances and assets is a critical element in securing a maritime environment that conventional people- and paper-based approaches are simply too costly and inefficient to fulfill.
- **Unable to accommodate the increasing use of information technologies.** Even before the ISPS was adopted, governments around the world had begun to require ports and vessels to implement security measures that rely on information technologies.¹⁰ A business or agency that fails to take steps now to build an infrastructure capable of accommodating the growing use of technology will find it difficult to change and grow as fast as its technology-proficient competitors.
- **Inflexible in response to additional legislation.** It is likely that the mandates described in the ISPS represent first efforts by the IMO and its contracting governments to produce legislation that will reduce the likelihood of a successful terrorist attack. Ports and vessels must work now to create a foundation that will be able to provide for additional security measures in the future – a requirement that point-oriented solutions, which drive up operational costs and lead times, are simply too inefficient and unmanageable to fulfill.

Conventional approaches are no match against the security and safety considerations unique to maritime applications. Companies and agencies will need to adopt a new approach to security and safety if they are to effectively protect waterways and the cities and populations that reside alongside them.

Our Philosophy, Our Solution

The good news is that a solution does exist that meets the challenges of securing assets and people in a maritime environment. At Ingersoll-Rand, we have developed an approach that both improves security and safety while also enabling our customers to reduce costs and improve productivity. It's a process we call **Integrated Security (IS)** and we expect it will help our maritime customers improve their operating efficiencies as it has for the dozens of Fortune 500 companies and government agencies that comprise our mainland customers.

At the heart of *IS* is the process of integrating 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

¹⁰ For instance, vessels moving cargo into the U.S. are required to forward a description of their contents electronically to relevant agencies before they are allowed to dock at a port.

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.

Integrated Security connects 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 replace paper forms of I.D. and significantly reduce the number of security personnel required for security screening. Because the architecture is open, the system easily accommodates 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. (See Table 1. on the next page for specific differences between *IS* and conventional systems.)



A crucial difference between conventional approaches and *Integrated Security* is the focus that *IS* places on improving efficiencies. Conventional security and safety systems are designed as an answer to the question, how can I improve security and safety? *Integrated Security* supplies the answer to this question and one other: How can I run a better, more productive business? It helps businesses operate more efficiently in four fundamental ways:

- ***IS* improves the management of information.** *Integrated Security* facilitates the collection and exchange of data between security and non-security related technology systems. It therefore acts as a tool that improves the effectiveness of various business processes. For instance, human resources managers can use data from a time-and-attendance system to track levels of tardiness. A CCTV application may produce data that can be used in connection with an inventory-tracking program.
- ***IS* increases cost efficiencies.** Because every system involved in *Integrated Security* is connected through a shared technology infrastructure, *IS* can be used to detect, investigate and resolve security violations far more quickly and with fewer security personnel and other resources than unconnected technologies. Resolving security breaches is therefore far more cost efficient as well as reliable using *IS*.
- ***IS* saves time.** *Integrated Security* is designed specifically to facilitate the seamless movement of people, cargo and equipment through entrances and other security points. Rather than requiring authorized individuals to endure the process of giving sensitive or even personal information, such as a Social Security card, to security personnel, *IS* relies on electronic-access cards coded with an electronic code or biometric identifier. For pre-screened employees, vendors and other individuals, the result is fast, hassle-free access, when and where they need it.

- IS becomes more efficient and reliable as it expands.** Perhaps the most significant difference between conventional approaches and *Integrated Security* is that *IS* becomes more effective as a security and business tool as it evolves. With each new opportunity to collect and leverage data, *IS* becomes better able to manage the people, openings and assets involved in a facility's operations. For instance, a new time-and-attendance application may generate data on employees that facilitates faster and more dependable verification of identity for authorized employees by means of an existing access-control system.

Table 1. Comparison between conventional security systems and <i>IS</i>	
Conventional Security	<i>Integrated Security</i>
Focus on restricting access at particular entrances and assets.	Focus on engineering facility-wide security systems.
Uses people and paper to govern specific openings and assets.	Uses integrated information technologies managed at a central location.
Limits access by unauthorized people at specific openings and assets – cumbersome and time consuming.	Facilitates seamless movement of authorized people throughout a facility when and where they need it – efficient and hassle free.
Relies on people screening paper forms of I.D. that can be lost, stolen or forged – unreliable, inefficient and difficult to change.	Uses access cards with electronic codes or biometric identifiers that would be highly difficult, if not impossible, to replicate – fast, efficient and reliable.
Relies heavily on the expertise, judgment and inclinations of security personnel.	Relies on trustworthy, rule-based systems.
Subjects each person to a similar security screening process regardless of her or his level of authorization.	Access granted for each employee's individual authorization level, as recorded in an access card, and by the facility's MARSEC level.
Tracks assets and personnel using disparate, unconnected systems.	Tracks assets and personnel using a single, connected database.
Security systems are point-based – they each have their own procedures and processes.	Systems are fully integrated to promote greater reliability and efficiency.
Relies on several vendors working on different applications – no single point of accountability.	Employs a limited number of vendors partnering to achieve a common strategy.
As systems grow, they become more decentralized and less manageable.	Easily accommodates expansion. As systems grow, they become better able to promote efficiencies and dependability.
Point-based security systems are never fully integrated into other business operations.	Security systems are integrated with other business operations. They become a tool for promoting innovation and enhancing overall business efficiency.

Integrated Security at Work in a Maritime Environment

Although *Integrated Security* provides clear benefits compared to conventional approaches for many industries, its advantages are especially pronounced in maritime applications. Examples of how *IS* can help a typical port and vessel enhance security and safety while also promoting efficiencies include:

- **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, *Integrated Security* combines time-and-attendance with access-control technologies to generate easily the required information when required.
- **Improve productivity of truckers.** Truck drivers typically have no way of systematically alerting a vessel's crew of their arrival time at a port. When they arrive, drivers must wait for crew to prepare cargo for transport – a poor use of time that likely adds up to millions of dollars in lost productivity for a typical shipping company. Using *IS*, registered drivers can electronically signal their scheduled time of arrival in advance so that when they arrive, cargo is ready for departure.
- **Automated response to different security levels.** If an emergency or threat to security arises, *IS* can 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, through *IS*, all major exits can open rapidly and automatically. For another threat, a *IS* 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, *Integrated Security* helps to 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 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. As an approach that relies on electronics and biometrics to verify identify, *IS* can readily accommodate the seafarers, TWIC and other identification card requirements.

Conclusion

Conventional security and safety approaches are inadequate for the unique demands of a maritime environment. A new methodology, *Integrated Security*, is a solution that can overcome the limitations of traditional point-oriented approaches by replacing them with facility-wide integration. In the process, *IS* can optimize the reliability and value of today's CCTV, electronic-access control and other security and safety technologies while enhancing business efficiencies for companies and agencies involved in maritime trade.

Through *Integrated Security*, port and vessel operators will be able to meet the challenges of complying with the ISPS and other recently enacted regulations. Equally important, *IS*, far better than conventional approaches, can act as a foundation for accommodating a growing body of legislation and the industry's increasing reliance on technology. *Integrated Security* will help operators save costs now and in the future while also ensuring that a facility's people, openings and assets are secure – a solution that, more than any other, fulfills what today's maritime industry needs most.

###