

Strategic planning for effective port security

Gianni B. Arcaini, Chairman and CEO, Duos Technologies, Jacksonville, FL, USA

Port and maritime operations represent a challenge to the security of nations and the global economy. Global trade depends on maritime transport. The United Nations Conference on Trade and Development (UNCTAD) estimated international seaborne trade of 8.17 billion tons of goods in 2008 [1], representing 80 percent of international trade. Despite the importance of international ports to global commerce, there are few uniform standards for point-to-point control of security on containers, cargoes, vessels, and crews. The port security of a single nation remains at the mercy of the standards and procedures of other nations.

The threat

Public policymakers are aware that ports remain critically vulnerable, but both funding and government-led efforts to harden port facilities are lagging while the focus remains on threats to air travel. In February of this year, for example, a hearing of the U.S. Senate Homeland Security Appropriations Subcommittee [2] addressed the disparity between funding for air travel security and funding for other vulnerabilities. Senator Robert Byrd noted that the fiscal 2011 budget provided only level funding for port security, among other areas, while providing for investment in technologically advanced airport scanners.

Port owners are subject to a patchwork of regulations and initiatives while working to meet individual security goals. Portions of a facility are often leased to private terminal operators, who are responsible for their own security, and there may be shared public/private responsibility for a site. The result is a balkanized system of port security and operations management, with security concerns often secondary to issues of time management and convenience.

The quality of security personnel is another issue. While many ports require background checks on their own hires, local security guards, often supplied by outside agencies, introduce vulnerability to the port and rarely have the skills needed to use advanced systems. A Jacksonville police officer doing a routine check at the entrance to the Port of Jacksonville stopped a man who had been working as a security officer at the Port for one week. The man, a Brazilian national, had been denied permanent immigrant status in 2007 and was carrying both an illegal firearm and a stolen police badge [3].

Strategic planning and technology solutions

Although government entities may have slighted port security, the same cannot be said of private contractors. An array of technology-based port security applications has become available, addressing everything from access control to container scanning to night-vision surveillance of harbors.

The most common buyer behavior, unfortunately, is acquisition of mixed, uncoordinated tools without a matching overall security strategy. It is not unusual to see a site where a jumble of technology has been purchased, but either never deployed or under-utilized, often due to its failure to integrate with existing systems. It is not surprising that the results for these applications often fail to meet expectations. Deploying multiple, independent tools yields a result that is less than the sum of its parts.



While government funding remains focused on airport security, ports are left vulnerable.

So, how does a “leading edge” port security solution turn into an ROI failure?

- When it fails to integrate with a defined security strategy and multi-year plan
- When it can only be used and managed by local personnel
- When it renders existing infrastructure obsolete or fails to take advantage of functional existing systems
- When it fails to supply real-time information to remote users, nor data that can be integrated with other applications for comprehensive analysis.

The optimal port security strategy is a scalable, multi-year plan that can be implemented in phased funding increments. It does not depend on aging technology and anticipates future technical developments. It examines existing systems to see where (or whether) they fit into the strategy, and always considers how new applications will co-exist with both existing and planned systems. By using a project timeline and strategic plan, the port is “shovel-ready” if grant money creates the opportunity to begin implementing a project sooner than planned.

By implementing an open-architecture, software-based solution, the port can avoid becoming tied to a single vendor. An integrated “smart” system creates a secure area by combining an array of cameras and sensors with detection algorithms driven by artificial intelligence software. This technology acts as a force-multiplier for the port’s security force and allows the addition of new, advanced layers of security. An integrated system leverages all technology and personnel investments by centralizing and correlating the inputs from multiple applications.

An automated intrusion detection system, for example, can be correlated with input from a “friend or foe” application to differentiate between an intruder and an authorized worker in a secure area. This system uses software to analyze video images and detect a human in the secure zone. Before the system generates an alert, it looks for input from an “active tag” carried by authorized personnel, and generates an immediate intruder alert if no tag is detected. Otherwise, it generates a conditional alert and allows

security personnel to compare the live image with a look-up image of the person's employee ID. If the data and image match, the security operator clears the alert. If there is no match, the operator responds per the customer's concept of operations (CONOPS).

This type of system allows authorized port personnel to monitor the system on a user interface in a network browser window, available from anywhere. When necessary, this allows simultaneous real-time sharing of information by multiple stakeholders. An automated intrusion detection system differentiates between actionable events and events without security implications. Port personnel respond only to confirmed incidents, armed with the information needed to resolve the event.

Video analytics: overcoming the myths

Although video analytics is not new, it is subject to several misconceptions that may get in the way of a strategic port security solution:

1. **The Black Box Myth:** The assumption that there is a standard solution that will magically meet all requirements.
2. **The Status Quo Staffing Myth:** The assumption that an investment in new applications does not require any change in personnel or hiring practices.
3. **The Fault-Free Myth:** The assumption that an effective security solution will never produce a false alarm.

The Black Box Myth

Although it seems obvious that no security solution is a magic bullet, buyers are still under pressure to deliver results. That can lead to short-changing the decision process, and committing to an application that solves one problem while creating others.

One size never fits all. While a standardized solution has the apparent benefit of quick implementation, even that advantage may be illusory. To be truly effective, a video analytics system must be tailored to the unique needs of the customer and the site, which includes the ability to integrate with functional existing systems. If a new application renders an existing system obsolete before its time, that's a net loss.

One of the best ways to assure a positive return on a technology investment is to assess how well it fits into the port's strategic security plan. That plan considers the unique requirements of the port's topography, its existing security infrastructure, funding sources, multi-year goals, and the need to coordinate among public and private stakeholders. It also contrasts the expected benefits of the application with the timing and ease of its implementation, which includes testing and user training.

The strategic plan also provides a way to deal with situations where a single, influential stakeholder champions an investment, convinced that it will meet a pressing need despite objections raised by others. With a plan in place, there is a rational way to test whether any proposed application meets the defined goals and investment criteria, without having to re-visit the plan every time funding becomes available.

The Status Quo Staffing Myth

Even the most advanced technology is only a tool to be used by trained personnel. An optimal result requires more than training for existing personnel; it requires a new kind of "soldier."

Technology-driven systems accept input from a range of sensors (including video cameras), analyze the data, and present the results to users. While this information facilitates good decisions, it still requires personnel who are comfortable using and responding to technical output. The quality of the response is affected by the quality of the personnel.



With video analytics, port personnel need only respond to confirmed incidents.

The potential for multiple, overlapping security events makes informed human judgment even more essential. If the system generates multiple event alerts, it takes a savvy user to determine the appropriate response. An overmatched responder is more likely to ignore the information and resort to past response patterns, which negates the investment and wastes resources.

If an investment in new technology is not matched with an investment in staffing and training, the new equipment may never be used or used only in a limited fashion that never meets expectations.

The Fault-Free Myth

In a detection system based on video analytics, there is an inherent trade-off between reducing false positive alarms and detecting all security events. No solution can detect all events without ever yielding a false positive, and there is a diminishing law of returns in pursuing that goal.

With the benefit of trained personnel who understand the technology, its limitations, and the conditions that may yield a false positive, an acceptable balance can be struck between false alarms and the risk of missing an event. The goal is to select the "least imperfect" technology that allows that balance to be achieved.

Port security best practices

A defined security strategy and a multi-year implementation plan offer the best chance of a positive ROI for technology investments.



Having a clear security strategy that is gradually implemented gives port authorities the best chance of getting a good return on technology investments.

The best-practices recommendation is the use of technology for 24/7 monitoring and intrusion detection and the use of trained personnel to interpret and respond to technology-based alerts. A balanced, effective approach employs an integrated, single point of command and control for all deployed systems at a port, including access control. An integrated system also supplies reports that can be analyzed to spot trends so management can move pro-actively to secure the port against a potential threat.

Video analytics has enormous potential to meet port security challenges, but it is still important to select a vendor who is willing to tailor a solution to the port's unique requirements and strategic security plan.

REFERENCES

- [1] UNCTAD, Review of Maritime Transport 2009.
- [2] "Napolitano faces questions about screening technology funding," SecurityInfoWatch, 25 February, 2010.
- [3] "Jaxport security guard was illegal alien," Jacksonville Times-Union, 3 February 2010.

ABOUT THE AUTHOR

Born in Milan, Italy, **Gianni Arcaini** was educated in Germany, Switzerland, and Austria. In the early 1990s, Arcaini formed Environmental Capital Holdings, also known as ECH, and then Duos Technologies, Inc., whose Chairman and CEO he has been since its inception. Mr. Arcaini is a respected authority on international and domestic security issues. He has appeared as a featured lecturer at the University of North Florida, as well as at numerous industry events and on discussion panels.

ABOUT THE COMPANY

Duos Technologies Inc., headquartered in Jacksonville, Florida, provides a broad range of sophisticated technology solutions with an emphasis on Homeland Security. Its systems are based on its proprietary object detection and behavioral analysis software.

ENQUIRIES

Gianni B. Arcaini
 Duos Technologies, Inc.
 6622 Southpoint Drive S., Suite 310
 Jacksonville
 FL 32216
 USA

Tel: +1 904 296 2807
 Web: www.duostech.com