

# Integrating Equipment and People for Seaports

Thanks to continued R&D efforts, the integration of old and new systems, as well as people and machines, is a much smoother experience than before.

BY CAMILLE SHIEH

The need to integrate various security systems for a seaport transcends from safety reasons to operational efficiency concerns. Installation and integration works can be challenging for solution providers as seaports operate almost 24/7, said William Moore, Business Development Manager for Oil and Gas, Schneider Electric. "Solution providers need to be able to work around the port schedule, and the best practice is to keep an open line of communication with the security committee and all parties at the port. For example, down time needs to be addressed when security measures are implemented."

Smooth and quick installations and integrations can be done when the operations team at the seaport is involved. "Once the needs of the security team, the operations team and other stakeholders are understood, it is much easier to select a security solution that meets most objectives," said Larry Bowe, President of PureTech Systems.

Among diverse choices, seaports particularly look for smooth, total site management. "There actually are best practices for continuous system integration that maintains backward compatibility while making new



**William Moore**, Business Development Manager for Oil and Gas, Schneider Electric

system capabilities available," Bowe said. "With the increased popularity of XML, interfaces between products and subsystems can be extended without breaking previous integrations. This method is sometimes referred to as loosely coupled integration. When engineered properly, systems can process the information they understand and simply ignore the information they don't understand. Existing functionality continues to work, and new functionality is available if the receiving system knows what to do with the new information."

Central management software, such as physical security information management (PSIM), takes full



**Ed Merkle**, Director of Port Security and Emergency Operations, Port of Virginia

advantage of this open system practice in order to make sense and use of the mass amount of data at hand. "The PSIM should not only integrate all systems on site for real-time data streaming, it should also connect to agencies outside the seaport, such as the National Oceanic and Atmospheric Administration (NOAA) for the U.S., for crucial and relevant information that affects seaport operations," said Ed Merkle, Director of Port Security and Emergency Operations, Port of Virginia. When a situation occurs, a PSIM solution should present SOPs based on the organization's policies and processes, said James Chong, CTO of VidSys.



“One weekend, the live feed from NOAA to our PSIM reported a thunderstorm warning 27 minutes before it was reported on the local news outlets, and the PSIM was able to guide the operator what should be done as preparatory procedures,” Merkle recounted.

### BOY WHO CRIED WOLF

Without exceptions, many perimeter and VCA setups at seaports produce false alarms. “The combination of basic perimeter fences with simple or smart cameras does not yield an adequate level of security in many cases,” said Hagai Katz, Senior VP of Marketing and Business Development, Magal Security



**Aluisio Figueiredo**, COO of Intelligent Security Systems

Systems. “Ineffective perimeter protection can create many false alarms, which, in addition to being both time-consuming and costly to verify, can cause security personnel to lose vigilance.”

Fine-tuning the entire system should be carried out during initial installation, and should be performed by a trained integrator, recommended Aluisio Figueiredo, COO of Intelligent Security Systems.

### BRIDGING THE PAST AND PRESENT

One way to facilitate the process of phasing out the old and bringing in the new is to use encoders and digital virtual matrix switches, Chong said. This kind of hybrid infrastructure is common for today’s seaports before becoming fully IP-based.

When migrating, vendors of older technologies/equipment may no longer be around, rendering APIs/SDKs impossible to get. The standard work-around is through dry contacts, but then the network and some functions might be lost, Katz said.

“Usually, we try to find out what the protocol is via analyzers and network sniffers,” Figueiredo said. “If this proves to be unsuccessful, we then use dry contacts and relays to integrate

such systems.”

In the U.S., if solution providers go out of business, the support organization that received the rights and ownership of the software for interface support would be reached, said Pat Kiernan, Marketing Director for the Americas, Nice Systems. “Almost all software providers have their code stored with a law office or similar entity as a protection for the customer in case of bankruptcy. It is usually a requirement in requests for proposal.”

“At the onset of a project, the seaport can request manufacturers to place designs in escrow that can be released to the port should they cease to offer a viable replacement or cease to exist,” Bowe added. “That way, the port can hire an integrator directly to maintain the applicable system component.”

Wouldn’t ripping out the old system and switching to a completely new system be better? This comes down to a cost/benefit analysis of the end user. “Of course, if there is no one available to support the system, then little choice is left but to replace the old system when it begins to fail,” Bowe said. Also, once the seaport security personnel notices video loss or distrust in the existing system,



it would be better to make way for a completely new system, Moore added.

For old equipment that is still up and running, Moore suggested moving it to a low-traffic, less critical area for a small cost without sacrificing security coverage. “The use of new technology in critical and high-traffic areas is highly recommended. With the advances made in HD, wide dynamic, megapixel and low-light cameras, seaports would be better off converting to better, newer technology.”

## DATA TRANSMISSION

For large areas, using 100-percent wiring equates high TCO for the seaport authority. Conversely, using completely wireless connections may lead to instability of signals and bandwidth restrictions. Most seaports today use a combination of both for maximum ROI and performance.

“Starting in 2001, we began putting in both wired and wireless connections at the Port of Virginia,” Merkle said. “We used wireless to support areas with insufficient fiber capability,

and it was less expensive, easier and faster to put in. However, wireless transmission is not as reliable, as there are still many disruptions during data streaming. In fact, for almost all areas we have converted to wired transmission.”

At many ports, wired transmission is used for places like the entrance, where many cameras need to be supported. The benefit of opting for wireless is the port’s ability to leverage the network connection for other nonsecurity systems, said Donal Colfer, Integrated Solutions Group Manager in the U.K., ADT Fire &

Security.

Increased usage of secured wireless technologies has been noted; however, bandwidth restrictions need to be taken into consideration, Chong said. “With LTE 700MHz frequency becoming available, there are wireless solutions that folks are beginning to try out. Yet, we will continue to see a hybrid of wireless communications and more traditional landlines for seaport environments in the near term.”

Wired or wireless transmission also affects the performance of so many new technologies now used by seaports. “For VCA to perform well, it needs sufficient video image quality and frame rate. If the connection from the camera to the command center is wired, the VCA processing can be performed anywhere along the connection,” Bowe said. “But if the connection from the camera to the command center hops across a wireless link at some point, it is best that the VCA be performed on the camera side, prior to the wireless hop.” This will afford it the best chance of successful image processing and notifications.



James Chong, CTO of VidSys

