Security Products

A Port's Priority

By Dr. Bob Banerjee · September 2007

Reliable security systems in U.S. ports are important in protectingphysical assets

ESTABLISHING dependable security systems at the nation's ports is no easy task. Significant challenges pertaining to both the ports' physical location and set up, as well as access to security data from remote locations, can complicate the installation and operation of security systems.

Physical obstacles, such as networking massive terminal facilities, and a lack of manpower for ongoing system monitoring and management often dictate the technological solutions available for ports. Such large installations also are traditionally accompanied with a hefty price tag, thanks in part to the labor required to install hundreds of miles of cabling for video surveillance, access control and intrusion detection systems. For many ports, which often have facilities spanning thousands of acres of waterfront, the ability to adopt a centralized security system approach can sometimes prove prohibitive without the appropriate technology.

Diverse Demands

The Port of Greater Baton Rouge in Louisiana, one of the top 10 ports in the United States and ranked 32nd in the world in total annual tonnage, faced problems when it recently looked to update its own security system. Situated 230 miles from the Gulf of Mexico on the Mississippi River and the U.S. Gulf Intracoastal Waterway, it covers multiple facilities that span 85 miles of the Mississippi River and encompasses Ascension, East Baton Rouge, Iberville and West Baton Rouge parishes in its port jurisdiction.

While the specific needs of ports around the world vary widely, many of the core operational requirements remain the same: efficient and secure transport of cargo and the security of staff and visitors working within the confines of the port. For the Port of Greater Baton Rouge, that staff roster includes port employees, dock workers, truck drivers delivering or collecting cargo and the personnel of the many tenant companies with operations on port property—a large agricultural supplier, a flour mill, a coffee roasting facility, a bulk petroleum storage operator and a fructose sweetener transfer facility. The port also specializes in serving the Gulf Coast petrochemical corridor.

Terminal Security

To find a solution that would satisfy the diverse needs of all stakeholders, port officials brought on board local systems integrator Vanguard Technologies Inc. to conquer the logisitical issues of the port's main Mississippi River Terminal and Inland Rivers Terminal. Due to the distance between locations, Vanguard Technologies recommended a hybrid wireless- based IP communication and fiberbased system.

"We were working within some specific restraints, namely to provide a costeffective system that would allow key personnel access to security data from a number of locations. There are two separate terminals—the main Mississippi River Terminal and the Inland Rivers Terminal—that needed to be connected via a network," said Jerry Jones, president of Vanguard Technologies. "By using video over IP-enabled equipment from Bosch Security Systems, we were able to provide a reliable, cost-effective video surveillance system. That solution features live video over an IP network, data access to all field devices and remote power management tools that enable port executives and facility security officers to manage the installed devices from the internal network or through secured Internet access."

The installation comprised more than 50 fixed and PTZ cameras, with encoders strategically placed throughout each location. Connectivity to the cameras and encoders was provided via an IP network, including both point-to-point and point-tomultipoint wireless devices, as well as more than a mile of multi-mode, fiberoptic cable. The MPEG-4 solution enables the port to manage bandwidth across a large IP network.

Because of the widespread use of wireless transmission, protection against intermittent network connectivity also is built into the system with the use of encoders with 2 GB of storage. If network connectivity is lost, recording at the edge continues. Once connectivity is restored, the central NVR tracks any gaps in the recording and automatically replenishes the missing pieces with the stored video.

The system uses long-distance video data packet transfer to address distance, terrain and logistics without compromising data integrity or security. It also provides the capability to archive video data for retrieval in the future. Another important feature is the system's ability to continuously monitor security devices and network links via powerful network monitoring tools to ensure 24/7 uptime, as well as fast problem resolution. The result is that each authorized operator has instant access to live video from all cameras, as well as any new camera that may be added to the system. The archived video is stored centrally on four NVRs using several Terabytes of fault-tolerant RAID 5 storage.

Perimeter Protection

Because perimeter detection in a port environment is often another logistical challenge, video is an essential element to security, stepping in where fencing and gates would be impractical, if not impossible, along what is typically a port's largest expanse of boundary—the waterfront. In some instances, the waterside perimeter also can play host to other commercial vessels or recreational boaters in addition to shipping traffic. Along the landside boundaries, video also is crucial on the perimeter, as many ports are located immediately adjacent to urban areas. These areas provide ample cover and access to resources for potential terrorists looking to use the port as an escape route or as the target itself.

For the Port of Greater Baton Rouge, cameras trained on the Mississippi River feature video content analysis capabilities (VCA) to draw operators' attention to significant events and reduce the amount of video traffic sent across the network.

Using VCA at the edge, only alarm video is transmitted, such as a vessel moving up the shipping channel or an unauthorized ship present in the river. Once the analytics determine if the ship is a threat, an alarm notifies port security officers, and one of the PTZ cameras automatically tracks the vessel as it makes its way upriver to port facilities. This technology diminishes the amount of bandwidth required but enables all camera channels to be monitored effectively through intelligent video analytics.

The Future Of Port Security

Adding multiple layers of security to comply with a growing list of stringent regulations, most enacted under the Maritime Transportation Act of 2002, has forced ports to develop comprehensive security plans to qualify for federal funding. While the grant program—which has awarded $400 million annually for the past five years—has helped to reduce the costs of adding new technology, the grants don't specifically cover the ongoing expenses of adding new personnel, training or other recurring maintenance.

Currently, many of the country's ports are focusing on the safety of cargo entering the United States. These efforts look at not only the physical cargo and the shipping containers—more than 9 million cargo containers enter U.S. seaports each year—but also the identity and background of the more than 850,000 transportation workers who handle the cargo as it makes its way through the intermodal shipping system.

Ports have been anxiously awaiting the implementation of the most high-profile federal project, the TWIC program, which provides background checks and identification card issuance to port workers, truck drivers and others who regularly access the secure areas of a port. The rollout of the program, which was to formally begin in July, has been plagued with delays over the past two years, due in part to the development of the sophisticated IT infrastructure needed to operate the nationwide system.

The implementation of such a measure has already thrust access control measures at ports into the national

spotlight; however, video surveillance can play a large role here, too. Integrating card access systems or other access control systems with video surveillance arms port security personnel with a comprehensive picture of perimeter access points, particularly in sensitive areas of the port, where employing a 24-hour security officer is cost-prohibitive.

Video also provides a reliable method for the verification of alarms. A keyholder trying to badge into a sensitive area of the port sets off an alarm after the access control system denies his or her repeated attempts to gain access. With the use of video, security operators can know instantaneously if the situation is in danger of escalating or if the cardholder is a recognized, authorized employee with an expired card. Recorded video that captures an access control event also can be used forensically by port investigators or other authorities after an incident. IP video also makes the viewing of this information possible from anywhere—the security director's PDA when he's out of town, the desk of the port's executive director, or the monitor or video wall in the security operations center.

Using video in conjunction with an access control system, particularly one at a gate or security checkpoint, also can be used for license plate capture and analysis, as well as a record of trucks entering and exiting that gate. Using this video could prove helpful in tracking shipments from inbound trucks or for other inspection necessities.

Taking advantage of today's available technology—video surveillance, analytics and access control—in conjunction with other security measures already present in the maritime environment will ensure that ports remain a safe and secure part of the nation's critical infrastructure.

About the author

Dr. Bob Banerjee
Dr. Bob Banerjee is the product marketing manager for IP video products at Bosch Security Systems Inc. He can be reached at (717) 735-6637.

Back to previous page