A Building Block Approach to Security at Shipping Ports

Robert C. Huck*\textsuperscript{a}, Mouhammad K. Al Akkoumi\textsuperscript{a}, Samer Shammaa\textsuperscript{a}, James J. Sluss, Jr.\textsuperscript{a}, Sridhar Radhakrishnan\textsuperscript{b} and Thomas L. Landers\textsuperscript{b}

\textsuperscript{a}School of Electrical and Computer Engineering, University of Oklahoma, 202 West Boyd, Room 219, Norman, OK, USA 73019; \\
\textsuperscript{b}College of Engineering, University of Oklahoma, 202 West Boyd, Room 107, Norman, OK, USA 73019

ABSTRACT

With over 360 ports of entry and 20 million sea, truck, and rail containers entering the United States every year, port facilities pose a large risk to security. Securing these ports and monitoring the variety of traffic that enter and leave is a major task. To accomplish this, the authors propose a fully distributed building block approach to port security. Based on prior work accomplished in the design and fielding of an intelligent transportation system in the United States, building blocks can be assembled, mixed and matched, and scaled to provide a comprehensive security system. Network blocks, surveillance blocks, sensor blocks, and display blocks will be developed and demonstrated in the lab, and at an inland port. The following functions will be demonstrated and scaled through analysis and demonstration: Barge tracking, credential checking, container inventory, vehicle tracking, and situational awareness. The concept behind this research is “any operator on any console can control any device at any time.”

Keywords: Port Security, Security Control Centers, Sensor Fusion, Video Surveillance, and Distributed Architecture

1. INTRODUCTION

While “transportation security receives large federal funding streams, facility protection has been left hanging” [1]. 20 million sea, truck, and rail containers entered the United States and 29 million trade entries were processed by the United States Customs and Border Protection in Fiscal Year 2005 [2]. These vast numbers of sea, truck, and rail containers pose a tremendous security risk both from an economic and political perspective. With as many as 30,000 containers entering the United States every day, physical inspection of all cargo would effectively shut down the entire U.S. economy, with ripple effects far beyond the seaports [3]. Government funding for the facilities and ports at which these entries occur is limited, so there is a need for low cost scalable security systems.

1.1 History

After September 11, 2001, the United States government took measures to enhance security at port facilities. There are more than 36 public ports in the United States through which 95 percent of the overseas trade passes [4]. The Maritime Transportation Security Act (MTSA) was passed in November 2002 which recognized that ports “are often very open and exposed and susceptible to large scale acts of terrorism that could cause a large loss of life or economic disruption” [4]. Currently, freight coming into U.S. ports is “spot checked” upon arrival and stored in a container yard while awaiting the next mode of transportation. The unloading, staging, and storage of these containers require fleets of trucks, large areas of land for staging and storage, and countless numbers of transportation and security personnel to move and secure these containers. Today, video surveillance, vehicle detection, fences and gates, and foot patrols are the usual means for securing the port facilities. Through the creative use of technological innovations, more effective means to secure the transportation infrastructure can be achieved that will allow efficient and uninterrupted freight-flow operations for trade. This research will build upon the prior work that investigated aerial surveillance to enhance port security [5] and previous research that led to the fielding of a large scale Intelligent Transportation System (ITS) [6] to provide advanced capabilities that will enhance port security.

*rchuck@ou.edu; phone 1 (918) 660-3239; fax 1 (918) 660-3238; http://tcom.ou.edu

Proc. of SPIE Vol. 7480, 748006 · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.830079
Fig. 1. Port of Philadelphia and adjoining CSX rail yard. Location 1 is the dock area for ship loading and unloading, location 2 is the container staging area where containers are stored awaiting pick-up, location 3 is the CSX container storage area where containers are picked-up or dropped-off as needed by rail operations, and location 4 is the CSX rail line used for loading the train cars and building trains for departure [source of aerial photo – Google Earth].

2. CURRENT AND ENHANCED PORT SECURITY MEASURES

The authors’ previous work examined the security of large ports, like the Port of Philadelphia shown in Figure 1, which encompass large areas of land for the staging and storage of containers and other freight that are off-loaded from international carriers for U.S. consumption. The distance from the dock where the containers are off-loaded (Figure 1, location 1) to the point where they are loaded onto trains for shipment (Figure 1, location 4) is greater than 2 miles (3.2 km). In Mega ports like the Port of Long Beach, the distance could be greater than 4 miles (6.4 km). This distance is significant because the area is also used for the staging and storage of these containers (Figure 1, location 2 and 3, respectively). The following measures are in use today: Fences and gates, foot patrols, cameras, and vehicle detection. Enhancements to port security measures using available off-the-shelf technology should include high-definition video cameras and video detection and tracking.

2.1 Fences and gates
The first line of defense for any security measure is physical security. Fences and gates provide basic physical security, but there is not a means to detect breaches of these deterrents by themselves. Technology exists for passive monitoring of perimeters through the use of motion detection or similar devices, but these are not fool proof and therefore easily defeated.

2.2 Foot patrols
Roaming security patrols driving around in vehicles or on foot provide additional security measures. The frequency of these patrols and their routine can be calculated through observation and therefore overcome with time. Response from roaming patrols is faster than waiting to be dispatched, but still not entirely effective.

2.3 Cameras
Traditionally, video surveillance systems require many cameras to cover large areas, requiring large networks and great computation and manpower to analyze [7]. These cameras are either fixed or pan-tilt-zoom (PTZ) cameras, and they are either analog video or Internet Protocol (IP) encoded video. All the camera video is fed to a central security center for display on a single monitor or at best, a video wall. These camera systems provide situational awareness over a vast area and require constant monitoring by trained personnel. This process of manually monitoring many cameras is tedious, ineffective, and expensive [8]. Fixed cameras provide a “quick glance”, but the effective operation of a PTZ camera requires the operator to control the camera while viewing the video. This is less effective since the operator is not able
to view other camera feeds simultaneously. Automatic panning of cameras provides some relief, but over time, moving images blur and become less effective to the operator or observer if not focusing on the video image. There is an urgent need for enhanced computational capability to keep pace with the many “eyes” that are being installed and their required analysis [9].

The use of video to secure shipping ports is essential. Situational awareness of the vast staging and storage areas is time consuming and manpower intensive and leads to missed opportunities for detection and interdiction. Through the use of adaptive surveillance, selecting the right mix of cameras, angles, and Field-Of-View (FOV) is the first step. Employing object detection and tracking, object and color classification, alert definition and detection, database event indexing, and search and retrieval will enable the cameras used for security to be ‘smart, useable, and scalable’ [10]. Replacing older low resolution cameras with high-definition cameras will greatly improve the detection capabilities and require fewer cameras to cover the same area by increasing resolution at greater distances while zooming. Infra-Red (IR) cameras provide a whole new capability for surveillance and detection by turning night into day for the observer. Military applications of target detection and tracking using IR capabilities in missile seekers have been used for many years effectively.

2.4 Vehicle detection

Technology advances over the past several years have enabled vehicle detection and recognition to play a bigger part in security. The use of vehicle detectors: pavement loops, X-Band RADAR traffic detectors, and video detection, is well-suited for traffic signal timing and sequencing based on vehicle presence and therefore useful for monitoring vehicle entry and exit at port facilities. These triggers can signal the security officer to focus their attention to a particular video display when a vehicle presence has been detected.

2.5 Video detection and tracking

Video detection and tracking offer many enhancements to existing camera security measures by reducing the workload on personnel. This workload reduction is accomplished by alerting and identifying them to activity of interest and training them to that activity through camera selection for video display and highlighting. For this paper, video detection and video tracking is defined as follows: Video detection is the ability to identify objects in images that appear or disappear from selected areas of interest. Video tracking is the ability to locate and highlight objects that move with respect to the background. Video detection and tracking will be an area of further research in the next phase of the investigation.

Current research is being done on the process of acquiring video through different inputs and detecting stationary and moving objects present in different video frames. Vehicles and pedestrians are important objects to detect and identify when it comes to port security. A multi-object detection approach [11] uses a multi-view/multi-category object recognition detector to detect vehicles and pedestrians in video images. For every frame, model selection is performed to achieve tracking of moving objects. In the research performed by B. Leibe [11], two scenarios are explored: a typical surveillance-type scenario with fixed camera installations and a mobile scenario where the video is coming from the inside of a moving vehicle.

Another approach shows the development of an object tracking algorithm which is based on Bayesian estimation of dynamic layer representation [12]. These layers are extracted from real-time aerial and ground video to track vehicles and pedestrians. An object is found in one of five cases: new object appearance, object disappearance, moving object, stationary object, or occluded object. Extensive experimentation shows that the system provides good confidence and ability in detecting several objects simultaneously.

In the work performed by S. Calderara [13], the use of more than one camera to collect the input video recordings was investigated. A multi-camera system was designed for the purpose of tracking people and their normal and abnormal trajectories. Background suppression and an appearance-based probabilistic approach were used for the purpose of detection and tracking. Two types of cameras were used, both fixed and Pan-Tilt-Zoom cameras. The classification of person or not person is determined using background suppression that analyzes the geometric shape and size of the moving objects.

Vehicle detection studies vary in the use of technology and the mathematical analysis used for image processing. In [14], automatic vehicle detection can be achieved using infrared sensors that capture a binary image. This image is then processed and chopped into several segments. The segments are differentiated according to their histograms; if the histograms show a considerable number of pixels above a defined threshold, then the corresponding image probably...
contains the target. A fuzzy inference system then uses the feature sets given by the histograms to output a target confidence value.

In [15], automatic vehicle detection is characterized through statistical approaches that are based on local features found in the image. This novel approach shows great tolerance to geometric variances and partial occlusions which degrade the detection process.

3. BUILDING BLOCKS TO PORT SECURITY MEASURES

The benefits of ITS in terms of improving transportation network efficiency, enhancing safety and security, reducing congestion and travel delay, reducing incident response times, and increasing the efficiency of both transportation and emergency response agencies are well known for traffic application. These same benefits can be used to improve port operations and thus enhance security. A typical ITS is comprised of vehicle detectors including inductive loops, microwave detectors, and closed circuit television (CCTV) cameras, fixed and portable dynamic message signs (DMS), highway advisory radio (HAR), an advanced traveler information system (ATIS) which is often Internet based, remote weather stations (RWS), and a typically heterogeneous communications network that links the field hardware to system operators, transportation managers, and emergency management agencies. In most cases, system control is implemented in a centralized traffic management center (TMC) that co-locates the system operators, transportation managers, response agencies, and their dispatchers [16], [17].

A major concern for public planners contemplating the deployment of ITS is the high cost of these systems. Thus, it became necessary to consider alternative control strategies in order to reduce the overall system cost to a feasible level without compromising system performance and without degrading public perception of the services offered.

The notion of distributed ITS control has been studied previously in a few cases. For example, Dicaf is a completely distributed ITS architecture that addresses vehicle routing by providing dynamic, geographically localized congestion information directly to specialized navigation processors on-board traveling vehicles [18]. These on-board processors utilize the dynamic congestion data to perform optimal route selection in real-time. In the State of Wisconsin, distributed ITS control has been implemented by deploying a network of “local” TMC’s that each manage a jurisdictional region and share information throughout the network [19].

The authors’ research and deployment of a Statewide ITS Console is distinct from previous distributed control architectures in that it provides the complete functionality of a centralized monolithic TMC and does not require any specialized in vehicle equipment. Any single instance of the ITS Console is capable of functioning independently as a central TMC for the entire State. However, a unique aspect of this architecture is that a large number of these low-cost consoles are deployed to operate simultaneously in a fault tolerant peer-to-peer network. This results in a virtual TMC where the various system operators, transportation managers, and incident management agencies can remain geographically distributed in their current facilities throughout the State, but still enjoy most if not all of the benefits provided by a large, centralized TMC environment.

This Statewide ITS currently covers four geographically separated major metropolitan areas, and has a 20-year plan that will incorporate most of the rural highways and smaller metropolitan areas into the Statewide ITS infrastructure. As a minimum set of functional requirements, the ITS must provide:

- Incident Management – incident detection information relayed to traffic managers for verification, assessment, and timely dispatch of appropriate response teams.
- Work Zone Traffic Management – traffic volume, speed, and queue information relayed to traffic managers.
- Weather Information Monitoring – weather and pavement sensor information provided to traffic managers and road maintenance crews.
- Critical Infrastructure Monitoring – monitoring of airports, water ports, and major highway interchanges for detection of incidents or shutdowns.
- Commercial Vehicle Operations – afford ease of travel through the State by allowing electronically tagged vehicles to process credentials in motion and to be weighed in motion.
- Public Dissemination of Information - messages and alerts posted to dynamic message signs, a web-based ATIS, and a 511 traveler information system; near real-time still images posted to the ATIS.
To meet these functional requirements, a wide array of field equipment is being deployed, including dedicated fiber optic cables, communication network hardware, pan-tilt-zoom (PTZ) CCTV cameras to provide full-motion video for incident management, web cameras to provide low rate video and still images for public dissemination, DMSs, Remote Traffic Detectors (RTDs), and RWSs.

Design requirements for the ITS Console are driven by a philosophy which insists that a sufficiently privileged user should be able to log into an ITS Console anywhere in the State and

1) control any ITS device at any time,
2) see video or images from any camera at any time,
3) post warnings, alerts, or informatory messages to all ITS Consoles statewide at any time,
4) post warnings, alerts, informatory messages, or images to the public ATIS and 511 system at any time, and/or
5) provide video from any CCTV camera to designated public and private agencies at any time.

This philosophy is consistent with the National Cooperative Highway Research Program findings that “Interagency exchange of information promotes rapid, efficient, and appropriate response from all agencies” [20]. In addition, due to the critical nature of the system, it must be fault tolerant; localized failures should not preclude the system from performing the rest of its non-failed functions. If an ITS Console or an ITS device has failed, the rest of the operators and devices must remain functional.

Through its user interface, the ITS Console must provide a geo-referenced graphical representation of the State that shows major and secondary roadways and is both panable and zoomable. It must support immediate jumping to predefined views. Where available, aerial photography will be overlayed on the map display when the appropriate zoom level is attained. ITS devices must be depicted by graphical icons that indicate location, status, and type of equipment and, when clicked, provide full control of the equipment. Graphical icons depicting incidents and work zones must also be easily added, deleted, edited, and exported to the public ATIS and 511 system.

Some of the agencies that are connected to the statewide private network of ITS Consoles include Traffic Engineering and Maintenance Divisions, Division Engineers, Civil Emergency Management and Homeland Security, 911 dispatchers, Emergency Management Services, local and state police agencies, fire departments, the National Guard, and the Governor’s Office. Each authorized user at each agency is provided with an ITS Console that is connected through the private network to all other ITS Consoles statewide in a peer-to-peer network. A multi-tiered system of user levels and user privileges is implemented to manage access to system resources and mediate critical sections. The ITS Console provides an “instant messaging”-like capability whereby one user can gracefully request access to a system resource that is currently under the control of another user, although a higher privileged user can always preempt a resource from a lower privileged user when necessary. Any given user maintains their level and privilege structure when logging in to an ITS Console anywhere in the State.

Nominally, a full-function ITS Console provides video distribution functions and control of CCTV video cameras and Internet protocol (IP) web cameras, identification, reading, and posting of incident and work zone locations and information, and control of DMSs for directly disseminating a variety of information to drivers including the current state of incidents, congestion, and detours, critical weather alerts, evacuation routing, and AMBER (America’s Missing: Broadcast Emergency Response) alerts. Sharing of CCTV camera video signals between agencies is carried out as agreed upon in specific interagency memoranda of understanding. In addition to the full-function ITS Consoles, there are also limited capability “read only” consoles available to certain private entities, such as news media that have a need for access to traffic related information.

General public access to the information provided by the ITS is through a web-based ATIS and a planned 511 traveler information system, both of which will be automatically populated with data from the network of ITS Consoles. One unique aspect of the Oklahoma system is that the CCTV camera video streams are reserved for incident management and will not be available to the general public. However, a set of four IP web cameras will be co-located with each CCTV camera to provide near real-time still images for public consumption. Fully privileged ITS Console users have the capability to block the still images from individual web cameras in cases where public safety, privacy, or security are at issue. An independent network of microwave RTDs is being deployed by Mobility Technologies, Inc.
At shipping ports, fences and gates, foot patrols, cameras, and vehicle detection are the mainstays of port security measures. The next logical step is to enhance these capabilities using existing technology. Computational capabilities have increased to allow for near real-time video image processing. Research into tracking, correlation, and identification of targets using fixed and mobile cameras has produced quantifiable results [11]. With this ever improving video surveillance capability, proper care must be taken to protect the rights of the people under surveillance. This imaging capability is a source for great public concern over personal privacy and loss of control of the information leading to potential negative use (i.e., voyeurism, espionage, oppression, etc.) [21].

Based on experience from previous projects, these ITS designs and architectures can be applied to ports to create scalable building blocks to achieve port security requirements without sacrificing functionality for the future.

4. DEMONSTRATION PROJECT

This demonstration is designed to show the use and scalability of available off-the-shelf technology to augment security measures at a port facility by fielding an ITS like system at the Port of Catoosa. The proposed building blocks will be demonstrated, as well as how they will scale to provide security measures for today and future technology advances.

4.1 Tulsa Port of Catoosa

The Tulsa Port of Catoosa shown in Figure 2, near Tulsa, Oklahoma, is located on the McClellan-Kerr Arkansas River Navigation System. This system is a 440-mile (704 km) waterway linking Oklahoma and the surrounding five-state area with ports on the nation’s 25,000-mile (40,000 km) inland waterway system, and foreign and domestic ports beyond by way of New Orleans and the Gulf Intracoastal Waterway. Because of its south central location, the waterway is operational year-round, regardless of weather conditions. The waterway travels 440 (704 km) miles along the Verdigris River, the Arkansas River, the Arkansas Post Canal and the White River before joining the Mississippi at Montgomery Point. New Orleans is 600 miles (960 km) south. There are 18 locks and dams on the McClellan-Kerr. Each of these dams creates a reservoir, or what is called a navigation pool. The system of locks and dams can be likened to a 440-mile (704 km) staircase of water. In an average year, 13-million tons of cargo is transported on the McClellan-Kerr by barge. This ranges from sand and rock to fertilizer, wheat, raw steel, refined petroleum products and sophisticated petrochemical processing equipment.

4.2 The Network Backbone

A dedicated Gigabit Ethernet (GigE) network will be created in and around the port for the network backbone. Where dedicated fiber optic cables are not available, the backbone will be constructed using Virtual Local Area Network (VLAN) connections on a shared GigE network in cooperation with other port tenants. As in the 20-year ITS deployment plan, additional fiber optic cables will eventually be installed to allow for a dedicated network backbone over the entire port facility. Security devices are not connected directly to the GigE network since this would constitute an inefficient use of the GigE ports. Instead, 100 Megabit spurs will deployed in daisy chain fashion to transport data from one equipment location to another until the aggregate data rate reaches a level that is practical for connection to the GigE backbone. These aggregated GigE connections generally occur at communication huts where GigE switches are installed.

There are a number of off-the-shelf switches currently being manufactured that meet the operational temperature range requirements for installation in standard roadside communications cabinets. The capacity of the GigE network will allow all operators and security device traffic to move around the network and meet the system requirements as articulated in [8]. For this system, two-plus-two spare fibers are required for both the GigE network and the 100 Megabit network.

In areas where fiber optic cable is not currently available, wireless network links will be installed as a temporary solution. For these connections, the Motorola Canopy™ system was chosen and has thus far proven reliable for the
application. Access points will be installed on camera poles where fiber optic cables were available and subscriber modules will be installed at the remote devices. The Canopy™ system provides 6.2 Mbps of bandwidth point-to-multipoint with a range of two miles (3.2 km). By installing a passive reflector, the range is increased to greater than 10 miles (16 km), but communications are limited to point-to-point only. A single Canopy™ link provides device control simultaneously with acceptable video quality for either a single CCTV camera video stream or multiple IP web camera video streams.

The architecture of the distributed IP network is shown in Fig. 3. In addition to video streams, communication with devices including control and data acquisition for RTDs and RWSs is also performed over this network. Either a single port serial server or a terminal server is used to attach an EIA-232 or EIA-422 device to the IP network. The terminal server devices are IP addressable, off-the-shelf, and handle the protocol conversion from EIA-232 or EIA-422 to IP seamlessly.

4.3 The Operator Console

Each instance of the operator console is an off the-shelf, Intel-based PC type platform running under Microsoft Windows XP. A concerted effort has been made to base the software architecture on open source and public domain packages where possible in order to avoid costly and recurrent software licensing fees. The following packages are required to support the operator console main application software:
• Apache web server (the Apache Software Foundation, www.apache.org). The operator console main program is a web-based application that runs in a specially configured instance of the Microsoft Internet Explorer. However, at no time is it envisioned that any operator console will have access to the World Wide Web (WWW); rather, the application consists of a collection of pages that are sourced from the local Apache server resident on-board each individual console.

• PHP scripting language (the PHP Group, www.php.net). PHP is a hypertext preprocessor that facilitates web-based software development.

• MySQL (MySQL AB, www.mysql.com). MySQL is a popular, open source database server product.

• MapServer GIS (Regents of the University of Minnesota, mapserver.gis.umn.edu). MapServer is a CGI application that facilitates and supports the development of web-based geographical information systems (GIS).

Within this environment, the main application software was developed using a heterogeneous mix of Microsoft Visual Basic, Visual C++, JavaScript, and PHP. This software was developed such that each operator console is capable of functioning as a standalone Operations Center Console, of displaying analog and digital video, of controlling the CCTV cameras and DMSs, and of controlling, configuring, and acquiring data from RTDs, RWSs, and all of the other various sensors and detectors that have been deployed. The control system is completely distributed in the sense that, on a dynamic basis, any operator console is capable of controlling any device that it can communicate with.

It is also fault tolerant in the sense that any group of one or more operator consoles, when connected together through a network or a subnet thereof, will cooperate to provide control of all devices connected to the net on an instantaneous basis. This is accomplished by implementing a sophisticated message passing queue between all operator console instances that are mutually visible to one another. The network of operator consoles are peer-to-peer but not Ad Hoc. Each console runs a common software program and maintains a common database that includes complete information about all authorized operator console users and about all operator console instances. Database synchronization is maintained via the queue. In cases where a particular console is required to send messages to a second console that is currently offline or not visible, those messages are queued until the destination console once again becomes visible.
When a given console operator desires to take control of a certain device, the operator selects the device via a mouse click and a message is sent through the queue to all Operator consoles. If another user is already controlling the desired device, the operator is alerted by displaying the controlling user name, organization, and phone number. The requestor can contact the controller using a built in “instant messaging”- like facility and ask that the device be released. This provides for a graceful transfer of semaphores. In case the controller is nonresponsive, a user with a higher level can always preempt the device. This is useful, for example, if an incident occurs and a security officer wishes to view the incident but the controller is unavailable to release the camera. In such cases, control is released by a message through the queue and is then granted to the requestor by the software. All such transactions are performed with the use of messages transmitted through the queue.

A number of other benefits are realized through implementation of the queue structure. Command logs are maintained for records keeping and troubleshooting. All actions performed by all operators are maintained in a command log that is stored in the common database. Error messages are also logged in the database and are accessible remotely by system maintenance personnel. The queue system allows orderly control of all devices. All operators that are able to communicate with a device are also synchronized with other operators in contact with that device. This queuing system keeps the multiple operator console databases updated and maintains synchronization between them. In case an operator console is isolated due to, e.g., a backhoe cutting its connecting fibers, the queue for that console is immediately updated when the console is reconnected with the larger network. A system of time stamps prevents stale messages from corrupting the database of any given console when it is reconnected to the network.

User levels and privileges are defined to represent the type of agencies and their functions that use the system. Each operator can be assigned to any configuration of level and privileges and this information is stored in the common database. When administrators make changes to the level or privileges of a user, messages are sent through the queue to update all other console databases. Through this process, any operator can log in to any operator console and maintain their assigned capability to operate the system.

It should be noted that external monitors, including wall mounted plasma displays, can be controlled by the operator console through external TV tuners connected through terminal servers. This capability provides for on-the-fly configuration of a centralized Emergency Operations Center (EOC) at any given location when the need arises. Additionally, with this implementation, a remote EOC can be established using wireless links if fiber is not available at the desired location.

5. CONCLUSIONS

Today, fences and gates, video cameras, and security patrols protect the container storage yards of our ports. With the use of off-the-shelf technology, port security personnel can be provided with tools to enhance their capability. High definition video cameras and Infra-Red video cameras should replace existing low resolution cameras. In the near future, ‘smart’ surveillance capabilities will become available to analyze video to reduce the workload. This paper briefly described the main features of the statewide ITS that is currently deployed and introduced a novel distributed control architecture that has totally eliminated the need for expensive, centralized operations centers. The system seamlessly integrates both analog and digital video streams under a philosophy which insists that all devices be accessible from all operator consoles statewide at all times. A potentially large number of geographically distributed operator consoles are connected in a fault tolerant, dynamically reconfigurable peer-to-peer private network. This approach effectively realizes a “virtual operations center” that enables the involved agencies to remain geographically distributed in their current facilities and thereby avoids the substantial cost of a single monolithic operations center. As the need arises, the system also supports dynamic consolidation of personnel and resources to configure a centralized EOC on-the-fly in response to critical events.

REFERENCES

“The national strategy for maritime security,”


