UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

A BUILDING BLOCK APPROACH TO PORT SECURITY

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

ROBERT CHARLES HUCK

Norman, Oklahoma

2011

A BUILDING BLOCK APPROACH TO PORT SECURITY

A DISSERTATION APPROVED FOR THE

COLLEGE OF ENGINEERING

BY

Dr. James J. Sluss, Jr., Chair

Dr. Mark B. Yeary, Co-Chair

Dr. Randa L. Shehab

Dr. Pramode K. Verma

Dr. Monte P. Tull

Dr. Sridhar Radhakrishnan

© Copyright by ROBERT CHARLES HUCK 2011

All Rights Reserved.

Dedication

I dedicate this accomplishment to my wife Erika. Her love, continued support, tremendous patience, and constant counseling has enabled me to finish.

Acknowledgments

The inspirations of many and the challenges of a few have taught me so much more that what is represented here. While this document is the completion of my work, it is not the end of the friendships that have formed during my graduate work.

I wish to express my sincere appreciation to Dr. James J. Sluss, Jr. for all the guidance, freedom, and opportunity that he has provided as my advisor, friend, and as Padrino, which has enabled me to get to this point. To my committee members, Dr. Mark Yeary, Dr. Monte Tull, Dr. Randa Shehab, and Dr. Sridhar Radhakrishnan for mentoring and challenging me, thank you. To Dr. Pramode Verma, for all the growth potential that you have provided me, thank you.

To all my professors, colleagues, and associates, thank you for all the knowledge that I have gained from you, and especially to Mouhammad Al-Akkoumi, who was there to pick up the slack when I needed help, good luck and thank you.

This research program was partially funded by a grant from the Federal Highway Administration and the program was administered by the Oklahoma Department of Transportation. This project was federally sponsored under the SAFETEA-LU transportation authorization act elements 1734 and 1902. Program management was provided by Thomas L. Landers, Ph.D., P.E., Dean, College of Engineering, and Technical Project Management was provided by Sridhar Radhakrishnan, Ph.D., Director, School of Computer Science.

Table of Contents

List of Tables

List of Figures

Abstract

With the ever present threat to commerce, both politically and economically, technological innovations provide a means to secure the transportation infrastructure that will allow efficient and uninterrupted freight-flow operations for trade. 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. Currently, freight coming into United States ports is "spot checked" upon arrival and stored in a container yard while awaiting the next mode of transportation. For the most part, only fences and security patrols protect these container storage yards. To augment these measures, this research proposes the use of aerial surveillance vehicles equipped with video cameras and wireless video downlinks to provide a birds-eye view of port facilities to security control centers and security patrols on the ground. The initial investigation demonstrates the use of unmanned aerial surveillance vehicles as a viable method for providing video surveillance of container storage yards. This research provides the foundation for a follow-on project to use autonomous aerial surveillance vehicles coordinated with autonomous ground surveillance vehicles for enhanced port security applications.

Cost is a major issue for security deployments at shipping ports. This research also introduces a novel distributed control architecture that has eliminated the need for expensive management centers, thereby dramatically reducing the overall system cost. Fault tolerant, dynamically reconfigurable peer-to-peer networks of low-cost geographically distributed security consoles operating under the philosophy that any console should be able to control any system resource at any time seamlessly integrate video streams from the various port areas.

To accomplish this, a fully distributed building block approach to port security is demonstrated. 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 are developed and demonstrated in the lab, and at an inland port. The following functions are 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."

Chapter 1 - Introduction

While “transportation security receives large federal funding streams, facility protection has been left hanging” [1]. Over 20 million sea, truck, and rail containers entered the United States and more than 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].

With Government funding for the security at shipping facilities and ports limited, there is a need for innovative, low cost, and scalable security systems. With the massive numbers of sea, truck, and rail containers entering the United States every year, these facilities pose a large risk to security. Securing these facilities and monitoring the varieties of traffic that enter and leave by different modes of transportation is a major task.

To accomplish this:

- Research into the development and fielding of a low cost fully distributed building block approach to port security at the inland Port of Catoosa in Oklahoma [4] was conducted.

- Work was also completed in the areas of autonomous surveillance vehicles, container monitoring and tracking, and network architectures to support these functions.
- To augment security measures, the use of aerial surveillance vehicles equipped with video cameras and wireless video downlinks to provide a birds-eye view of port facilities to security control centers and security patrols on the ground was investigated. This initial investigation determined that the use of unmanned aerial surveillance vehicles was a viable method for providing aerial video surveillance of container storage yards. This research provided the foundation for a follow-on project to use autonomous aerial surveillance vehicles coordinated with autonomous ground surveillance vehicles for enhanced port security applications.
- Based on work accomplished in the design and fielding of an Intelligent Transportation System (ITS) in the United States [5], functional building blocks, (e.g., Network, Camera, Sensor, Display, and Operator Console blocks) were assembled, mixed and matched, and scaled to provide a comprehensive port security system. The concept behind this project was "any operator on any console can control any device at any time."

Protecting the United States, the commerce that drives the economy, and the entities that ship and receive, requires many pieces integrated into a comprehensive system of security. This documents the completion of a project on Intermodal Containerized Freight Security. Through this work and separate work accomplished by other team members, research into several types of technologies available for security was accomplished, a demonstration of container tracking devices and surveillance options was conducted with cargo containers, and finally, the development and deployment of a low cost security system at the Port of Catoosa in Tulsa, Oklahoma was accomplished.

This architecture is unique from known existing systems providing security at shipping ports and is an enhancement to the previous ITS work by mandating that all functionality come from database queries. This architecture provides scalability through building blocks, like Lego® building blocks, that can be stacked and interlocked, mixed and matched to form a design to cover the particular aspects of the environment where the system is to be deployed.

According to the International Council on Systems Engineering (INCOSE), "Systems Engineering is an interdisciplinary approach and means to enable the realization of successful systems." This research followed a systems engineering approach as appropriate to the phases of this project. The phases of a systems engineering approach include: Operations, Performance, Test, Manufacturing, Cost and Schedule, Training and Support, and Disposal. Because of the short nature of this research, not all phases were considered, and will be left for future work.

1.1 Research Goals

The main goal of this research is to demonstrate that commercially available off-the-shelf technology can be used to augment current security measures at shipping port facilities. Additionally, by developing a structured, well designed, and simple software implementation, these off-the-shelf technologies can be deployed, multiplied, and integrated at a minimum cost to the port facility while reducing the software maintenance costs associated with system evolution. Simple software adapters know as ActiveX controls and terminal servers to connect non-network enabled equipment and legacy equipment to the network can be used to allow integration of existing systems.

To accomplish these goals, a distributed architecture is employed, where each console is stand-alone, yet integrated into the network and system.

Many operators can be connected to the system without interrupting other operators. Many devices can exist on the system, additional devices can be added by updating the database through provided Graphical User Interfaces (GUIs).

The premise of this system design is – Any operator can control any device at any time to access any information needed to accomplish their mission. Whether at the Port of Catoosa, in Washington DC, or in an Emergency Operations Center, the operator has visibility into that facility.

1.2 Dissertation Outline

Chapter 2 is a look at the current state of security at several of the larger shipping ports in the United States. While attending an ITS America conference, the tour of the Port of Philadelphia provided an invaluable insight into the interworking of a large shipping facility and their adjoining intermodal rail facility. In Chapter 3, the results of Phase I of the Intermodal Containerized Freight Security project as it relates to this research are discussed. The outcome of this phase was the development of plan to demonstrate several security measures that can enhance existing port security measures.

Chapter 4 addresses a video surveillance concept that was submitted to the Tulsa Port of Catoosa for consideration. The proposal was to go forward to the Fiscal Year 2007 (FY07) Infrastructure Protection Program (IPP) Port Security Grant Program (PSGP). Chapter 5 covers the events accomplished during Phase II of the ICFS Program as related to this research. Specifically, this Chapter covers the completion of the demonstration program at the Port of Catoosa and the aerial surveillance vehicle operations.

In Chapter 6, the design of the system's building block approach to port security is described. Chapter 7 is a discussion of the deployment of the system. In Chapter 8 the software architecture that was instrumental to the success of the program is described. Chapter 9 covers the hardware that was deployed at the Tulsa Port of Catoosa. Chapter 10 is a summary of the results of this research and the deployment at the Tulsa Port of

Catoosa. The Conclusion is addressed in Chapter 11, and Chapter 12 covers a few areas for further research.

Chapter 2 - Background

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 [6]. 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" [6]. 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 foot patrols, fences, and gates 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 built upon the work that investigated aerial surveillance to enhance port security [7] and research that led to the fielding of a large scale Intelligent Transportation System (ITS) [5] to provide advanced capabilities that will enhance port security.

This work examined the security of large ports, like the Port of Philadelphia shown in Figure 2-1, 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 2-1, location 1) to the point where they are loaded onto trains for shipment (Figure 2-1, 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 2-1, location 2 and 3, respectively). At these large port facilities, cameras are added to the arsenal of security technologies in use. Enhancements to port security measures using available off-the-shelf technology should include high-definition video cameras and video detection and tracking.

Monitoring freight flow into and out of port facilities is one challenge: during the voyage across the ocean, through the inland waterway, and across the open highway should also be considered. Many proposed systems and subsystems from numerous vendors and supplies who tout their effectiveness are available.

Complete Systems **-** Many projects are available that appear to solve the whole problem but at what cost? For example, the Lockheed Martin Neptune system is designed to collect data from a ship's Automatic Identification System (AIS) and surface tracking radar to provide information about shipping lane activity. This data would be

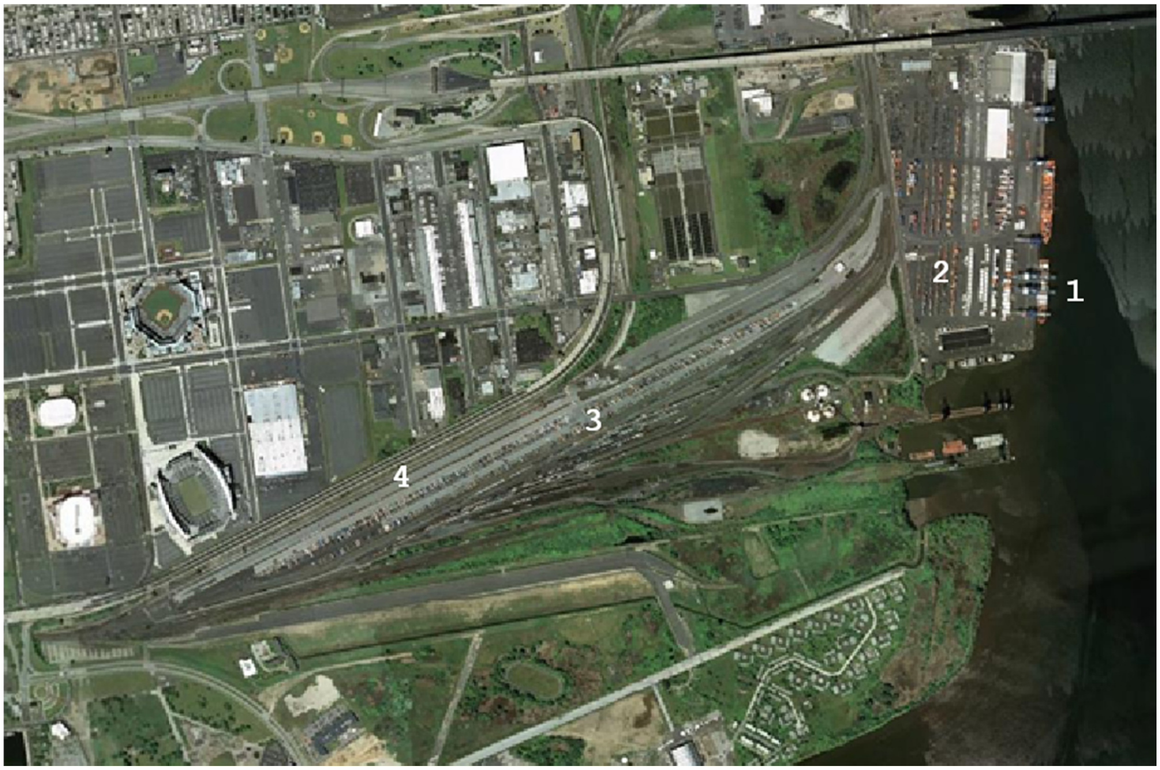


Figure 2-1. Port of Philadelphia and adjoining CSX rail yard.

(Image Source – Google Earth)

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.

transmitted to a central facility and could create an up-to-the-minute picture of maritime activity. Using this system, a 50,000-ton ship was tracked on a 45 day voyage and encountered and reported on 5,500 other ships [8]. This system is a potential way to track ships while underway or in port, but what about the cargo before it is loaded on the vessel? What about the containers after they are unloaded, or while in transit to their final destination? Some major trucking companies use Global Positioning Systems (GPS) on their truck fleet to track truck location; these devices provide information about their fleet location. Was the cargo door opened while in-transit? Did the cargo exceed the temperature threshold causing spoilage?

Individual Components - There are several off the shelf technologies that are readily available to fill in the pieces of a security system, but they all stand-alone without integration, i.e., no common interface, no common database, and no common control.

- Cameras - Traditionally, video surveillance systems require many cameras to cover large areas, requiring large networks and great computation and manpower to analyze [9]. 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 [10]. 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 [11]. 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 fields-of-view 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’ [12]. 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.

- 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.

- Video detection and tracking - Video detection and tracking offer many enhancements to existing camera security measures by reducing the workload on security personnel. This workload reduction is accomplished by alerting and identifying them to activities of interest and training them to that activity through camera selection with video display and highlighting. For this project, video detection and video tracking was 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 a potential future phase of investigation.

- Motion detection - Many COTS cameras have built-in motion detection capabilities and algorithms. They can detect and alert operators of movement during off hours and send emails or store images for later analysis. These are best suited for fixed cameras with fixed motion detection windows of interest. Newer PTZ cameras come with motion detection and tracking to follow the movement after detection, the same alerting opportunities exist as for fixed motion detection cameras.

- Sonar surveillance systems - The AN/SQR-17A Acoustic Surveillance System is a state-of-the-art COTS-based acoustic signal processing system used by the U.S. Navy's Mobile In-shore Undersea Warfare amphibious community for undersea surveillance. This system detects and provides acoustic threat data, monitoring surface ships, small boats, submarines, mini-subs and swimmer delivery vehicles [13]. By placing these devices in the shipping channels, detections can trigger alerts for further investigation.

The Container Security Initiative (CSI) of the U.S. Customs and Border Protection (CBP) agency was implemented to address security of shipping containers when they are not onboard a ship [2]. Many cargo container tracking options have been proposed by multiple vendors but no standard has yet been established. The Intermodal Containerized Freight Security project looked into the many devices currently in-use and proposed a solution as documented in Intermodal Containerized Freight Security Phase II Deliverable D.F.4 - Assessment of Container and Cargo Integrity Sensor Alternatives, written by Yogesh Varma and Dr. Monte Tull, part of the Systems Engineering Group, in 2007 [14]. This work is outside of the scope of this project and may be looked at further in future work.

Chapter 3 - ICFS Project Phase I

The purpose of Phase I was to identify two representative scenarios for the demonstration of surface and air surveillance of a shipping port. In order to accomplish this task, an investigation into shipping ports, their layouts, and their existing security measures was necessary. The systems engineering framework provides a formal process to define users' needs and specifies methods for developing the required functionality that was considered in this phase. The outcome of this Phase of the project was a Demonstration Plan, ICFS Project Phase I Deliverable T.F.3 [15].

The following ports were investigated as they represent a large volume of cargo into the United States: Figure 3-1 the Port of new York/New Jersey, Figure 3-2 the Elizabeth Marine Terminal, Figure 3-3 the Port of Seattle, Figure 3-4 the Port of New Orleans, Figure 3-5 the Port of Long Beach, and Figures 3-6 through 3-11 the Port of Philadelphia. Each of these ports presents their own unique challenges for port security.

The Port of Catoosa, near Tulsa, Oklahoma was chosen for the demonstration location. Because of the close proximity to the University of Oklahoma – Tulsa Campus, this was ideal. Working with the Port Authority also turned out well, as they were instrumental in the original funding avenue for this project. The Port is not large in tonnage but certainly large in land area and diversity of shipped goods, both into and out of the Port facility.

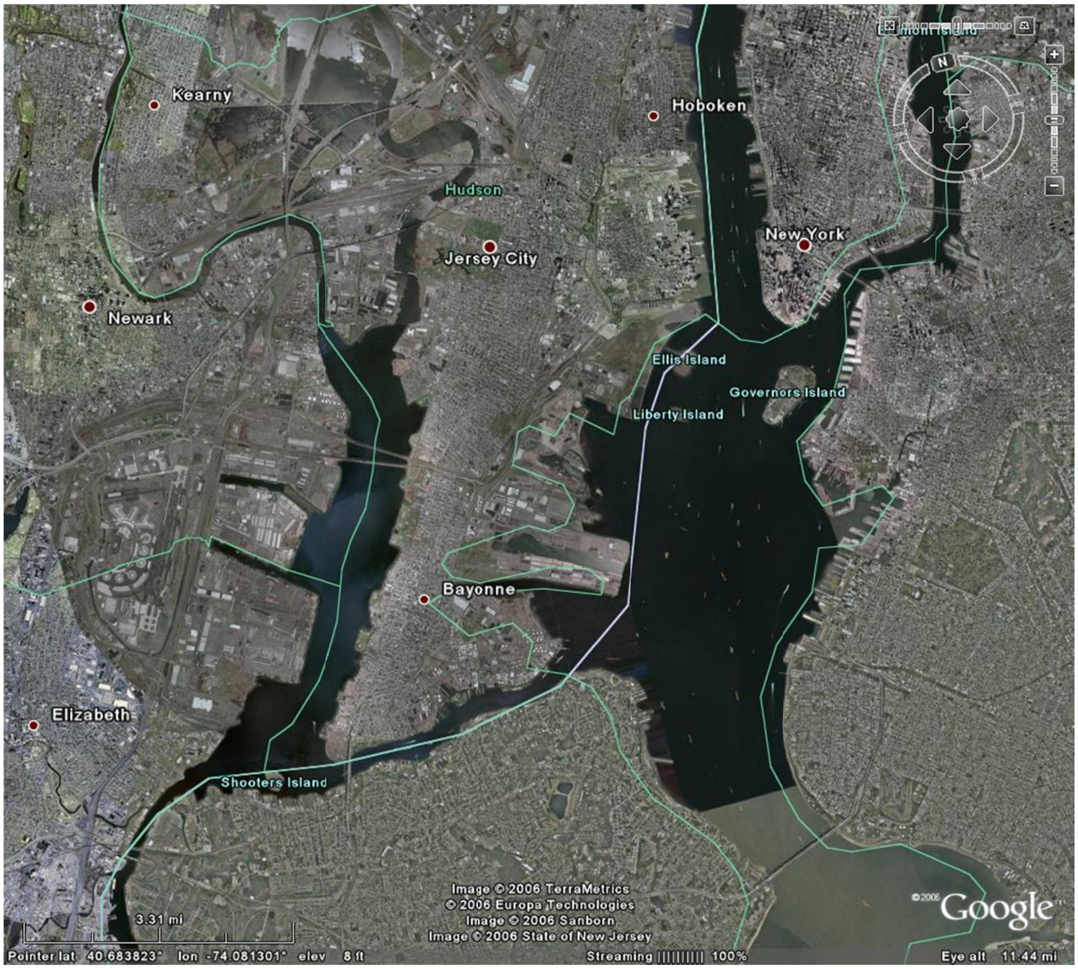


Figure 3-1. The Port of New York/New Jersey.

(Image source - Google Earth)

The port authority for the Port of New York/New Jersey has six port facilities under their jurisdiction. The six facilities include: Port Newark and the Elizabeth Marine Terminal which are the principal container ship facility for New York-Newark metropolitan area, Howland Hook Marine Terminal which handles containers only and has an on-site five-track intermodal rail facility, the Auto Marine Terminal for private auto imports and exports, the South Brooklyn Marine Terminal which handles mainly roll-on/roll-off and break-bulk cargo, and the Red Hook Container Terminal with six container cranes.

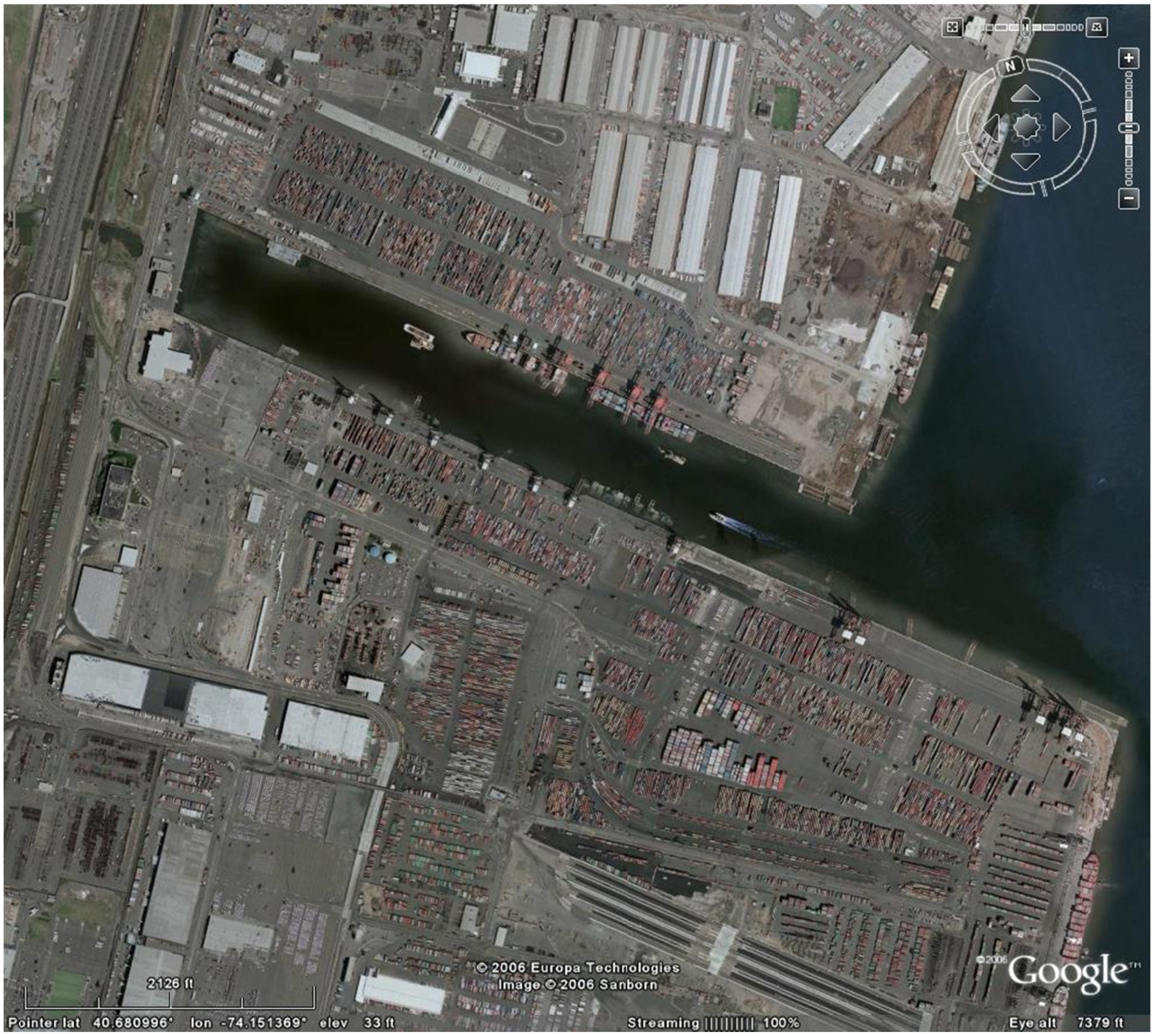

© 2006 Europa Technologies
Image © 2006 Sanborn
2126 ft
Pointer lat 40.680996° lon -74.151369° elev 33 ft
Streaming |||||||||| 100%
Eye alt 7379 ft
©2006 Google

Figure 3-2. Elizabeth Marine Terminal.

(Image source - Google Earth)

This port is located in Newark, NJ and is number one in volume of imports from Germany [16]. Elizabeth Marine Terminal is a large port from a cargo perspective, but small in land area. It handles a large number of cargo containers and has a rail yard included in the facility. It is challenging because it is located in a very densely populated area.

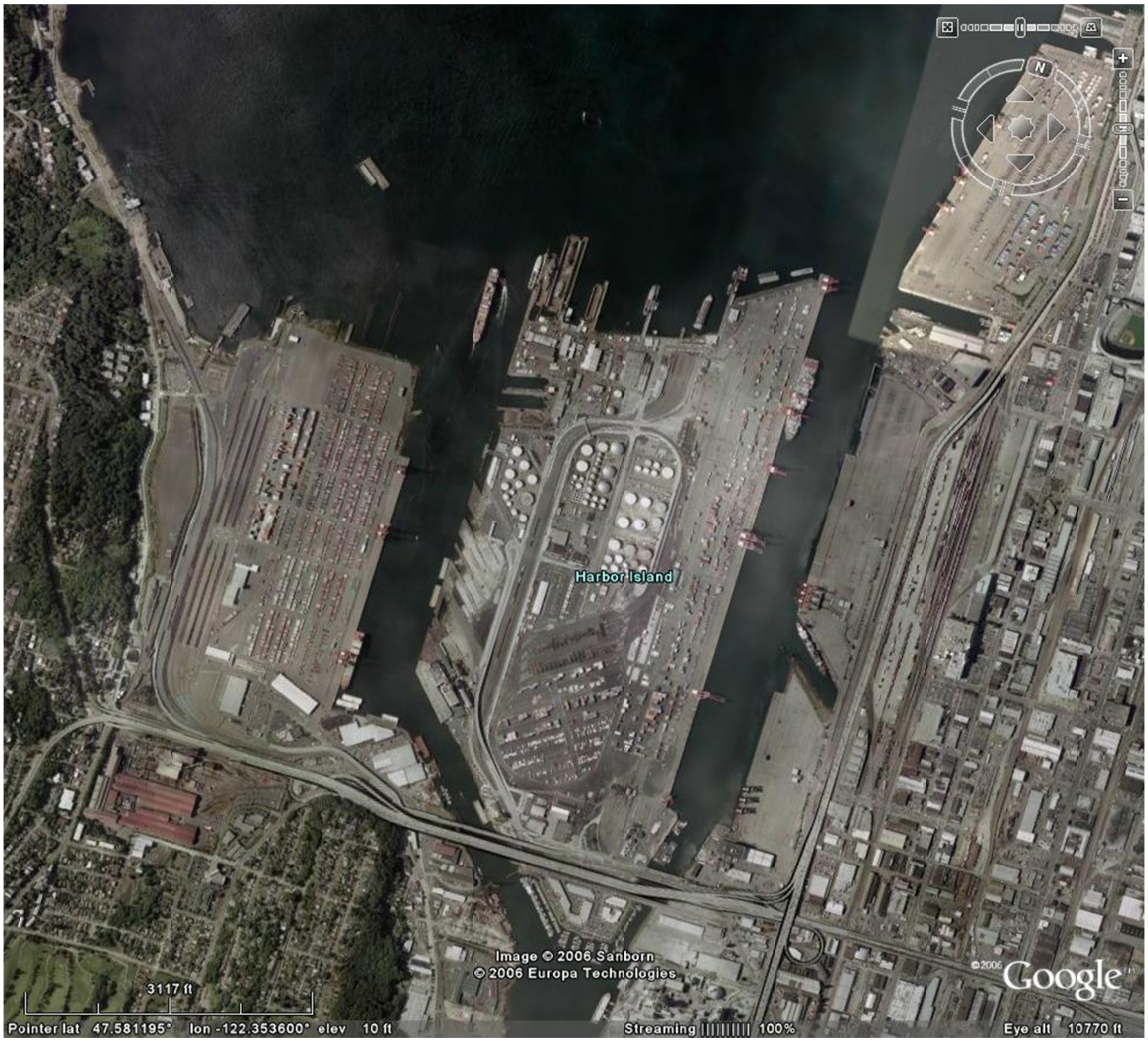


Figure 3-3. Port of Seattle.

(Image source - Google Earth)

The Port of Seattle and the Seattle/Tacoma Airport make up the Seattle Port Authority. The Port of Seattle handles a large amount of containers, more than 2.1 million 20-foot equivalent units (TEUs) in 2010 [17]. It is constructed on a private manmade island with an intermodal rail facility onsite.

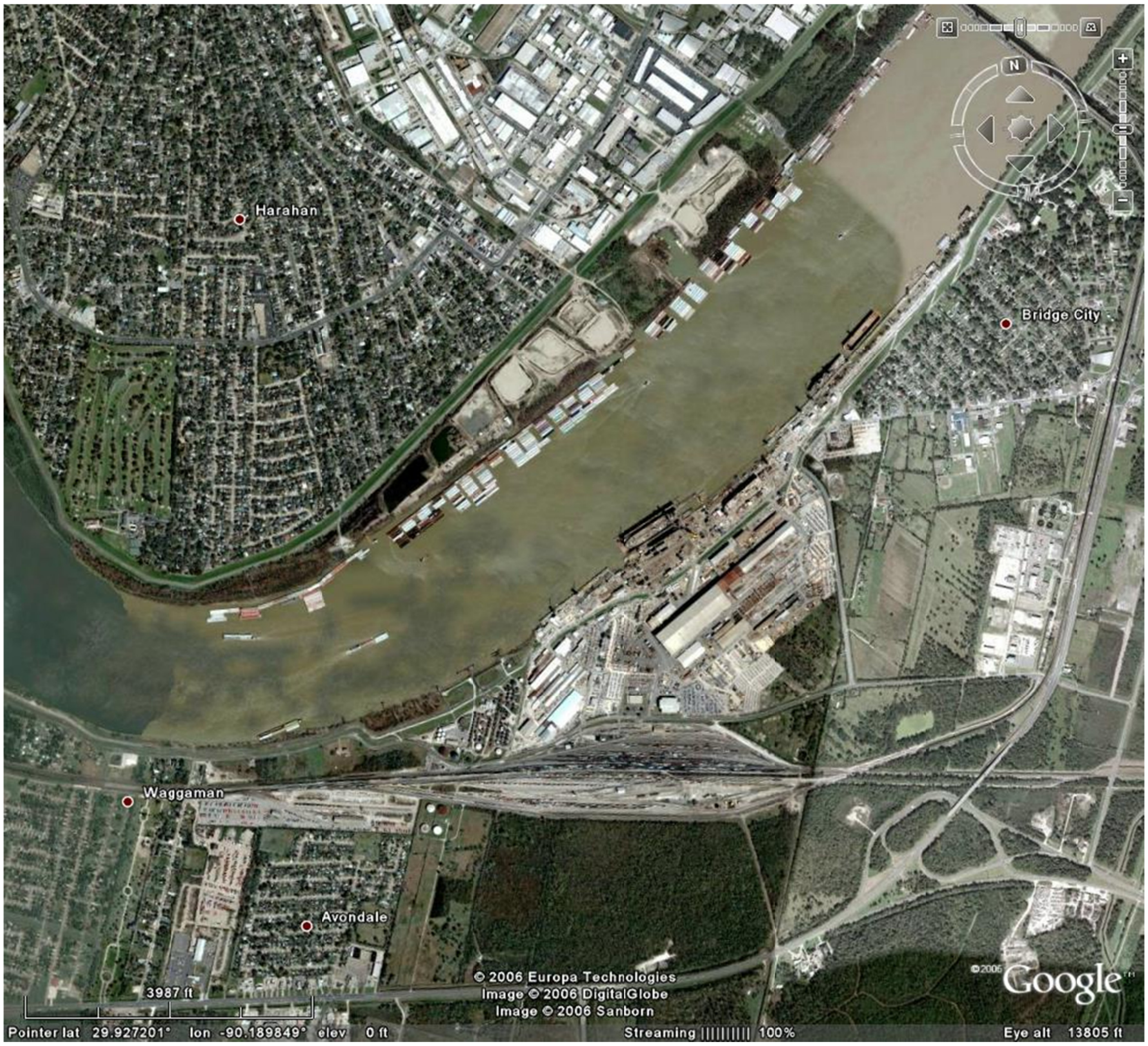


Figure 3-4. The Port of New Orleans.

(Image source - Google Earth)

The Port of New Orleans is uniquely located at the mouth of the Mississippi River making it strategically located to handle all container traffic and bulk cargo to and from the river. Large ships entering the Gulf of Mexico must transfer their cargo to barges that will transport their cargo to all shipping points in the central United Stated. Cargo originating at the Port of Catoosa makes its way down the Arkansas River to the Mississippi River then to Port of New Orleans.

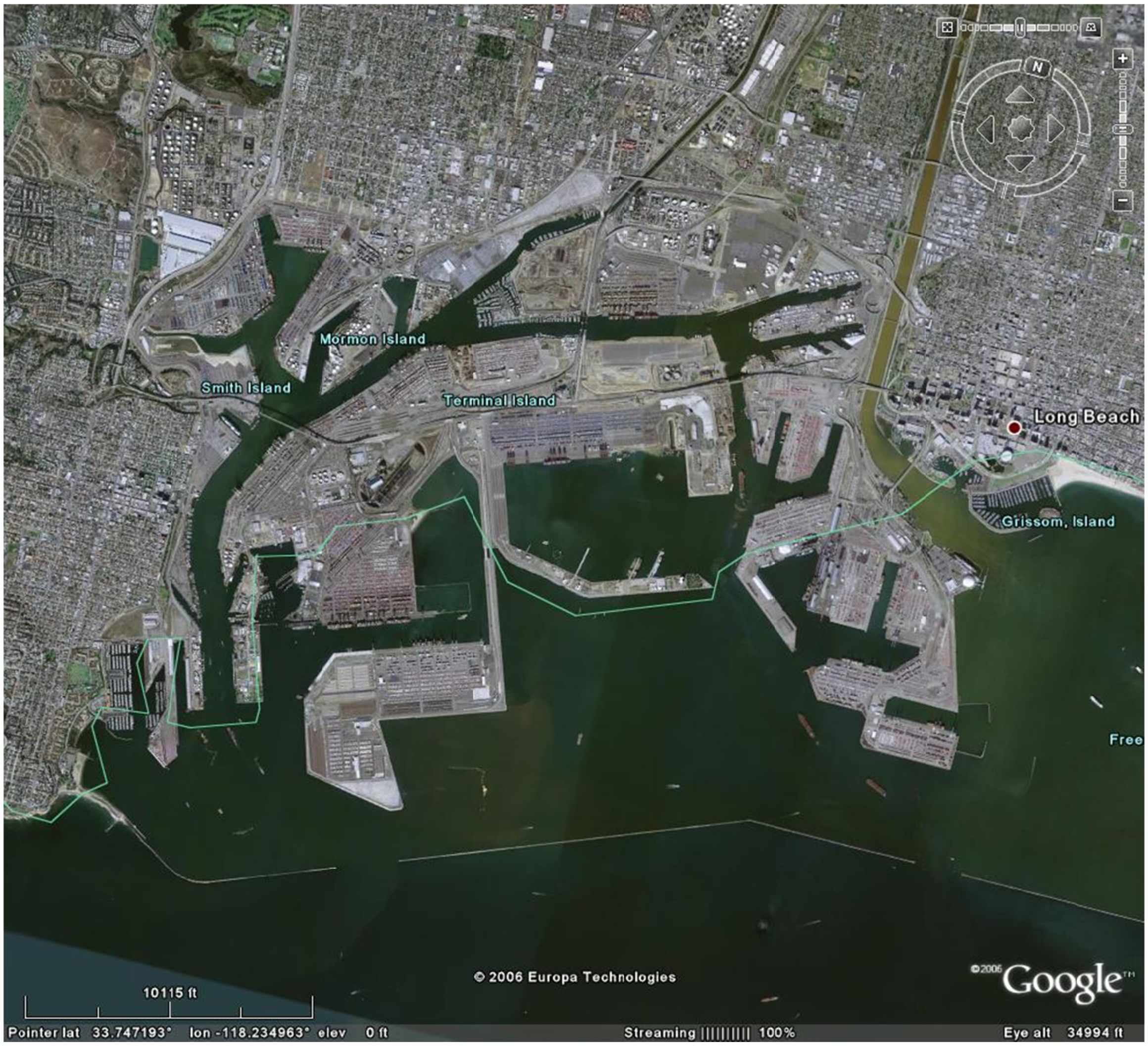


Figure 3-5. The Port of Long Beach.

(Image source - Google Earth)

The Port of Long Beach is large in land area, over 3,200 acres in size. It handles most cargo to and from Asia, nearly 6.3 million TEUs in 2011 [18]. The distance from ship terminal to rail facility is greater than 6 miles and presents many challenges, both from security of the storage yard and traffic onto and off the shipping terminal.

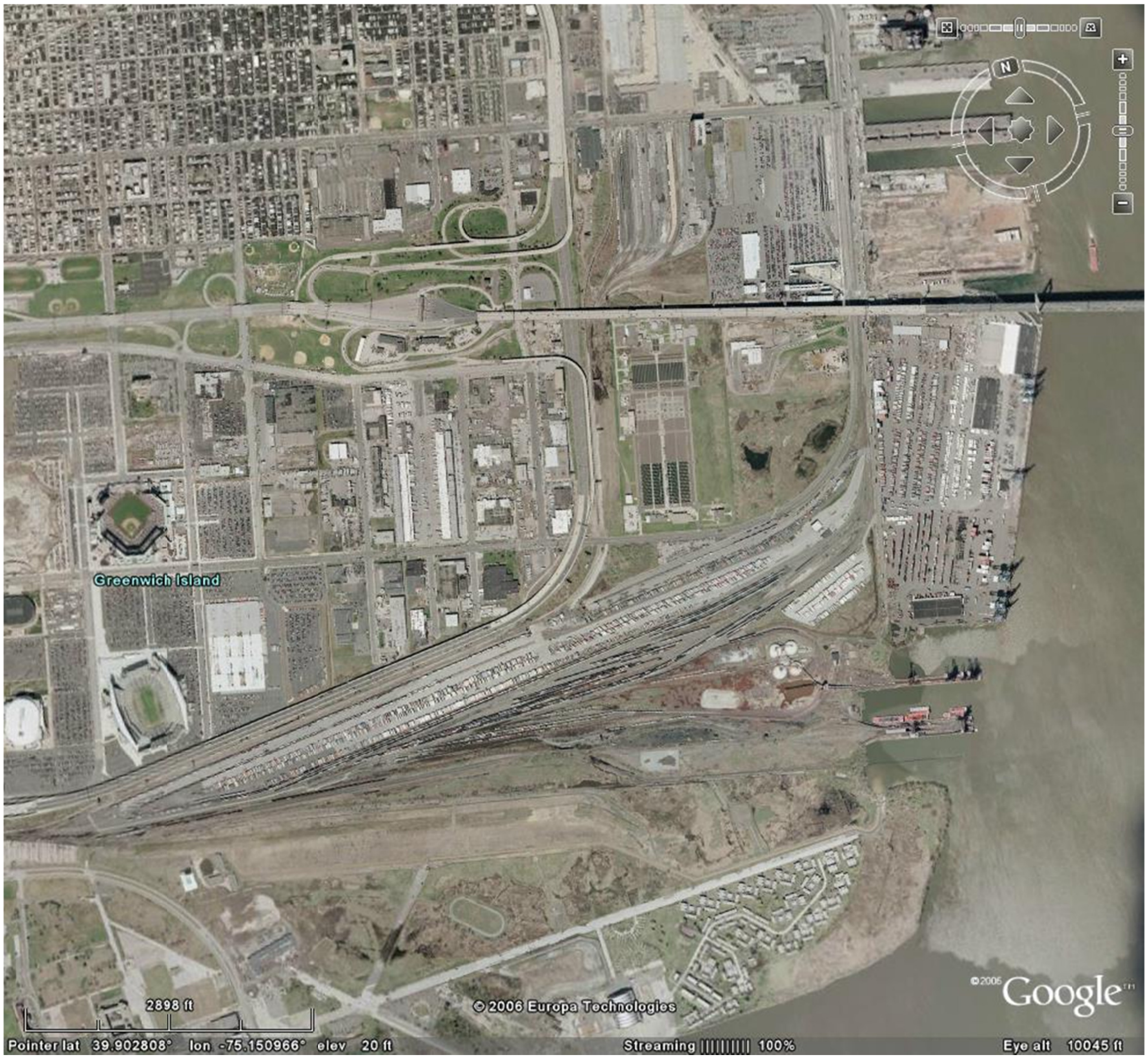

Greenwich Island
2898 ft
© 2006 Europa Technologies
©2006 Google
Pointer lat 39.902808° lon -75.150966° elev 20 ft
Streaming |||||||| 100%
Eye alt 10045 ft

Figure 3-6. The Port of Philadelphia.

(Image source - Google Earth)

The port of Philadelphia is a small port with large container traffic. Located on the waterfront near an NFL football complex and an NBA arena as well as many cruise ship birthing areas creates a lot of traffic in the area. The CSX railyard is across the street and most of the containers move out of the port through their yard.

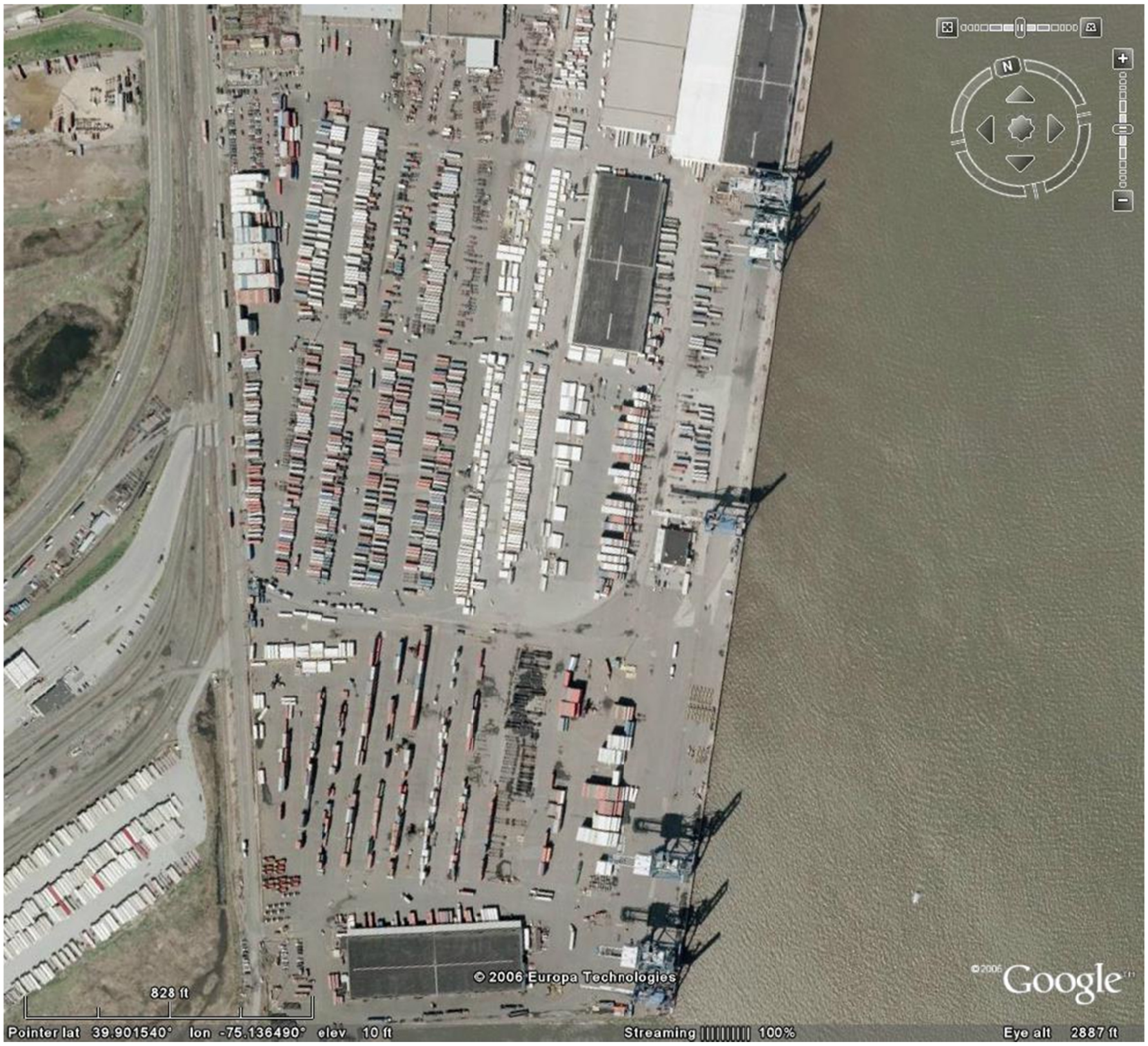

N
828 ft
© 2006 Europa Technologies
©2006 Google
Pointer lat 39.901540° lon -75.136490° elev 10 ft
Streaming ||||||||| 100%
Eye alt 2887 ft

Figure 3-7. The Port of Philadelphia Dock and Container Staging Area.

(Image source - Google Earth)

There are two container storage yards at the port. One on the port facility and the other located at the CSX railyard. Inspections of offloaded containers takes place in the port facility before being moved to the CSX yard.

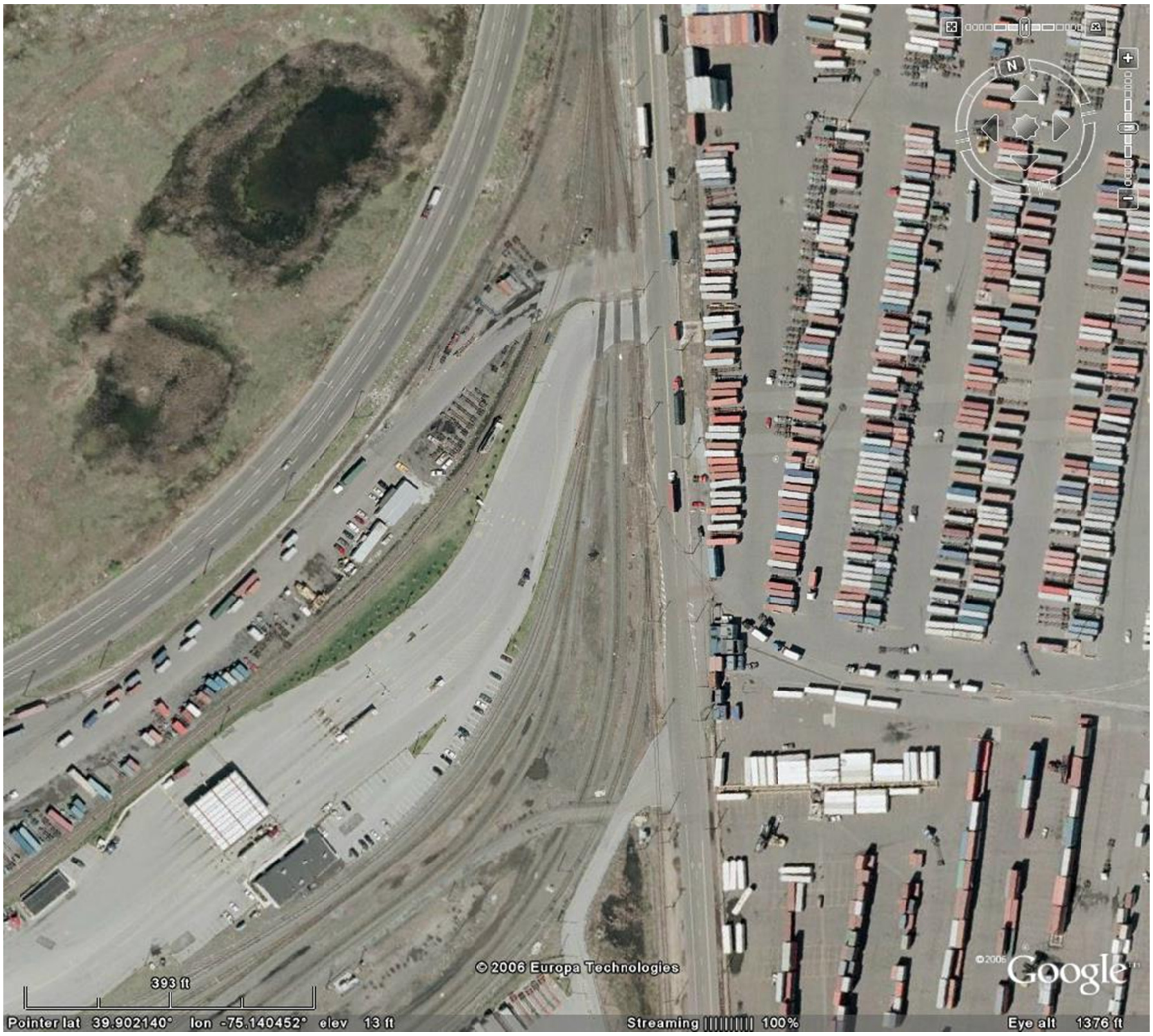

© 2006 Europa Technologies
393 ft
Pointer lat 39.902140° lon -75.140452° elev 13 ft
Streaming ||||||||| 100%
©2006 Google
Eye alt 1376 ft

Figure 3-8. The Port of Philadelphia enterance to the Rail Facility.

(Image source - Google Earth)

The containers are moved to the CSX railyard after clearing customs at the port. The containers are stored until they are either loaded trains for long haul journeys or picked up by the truck drivers for shorter distances.

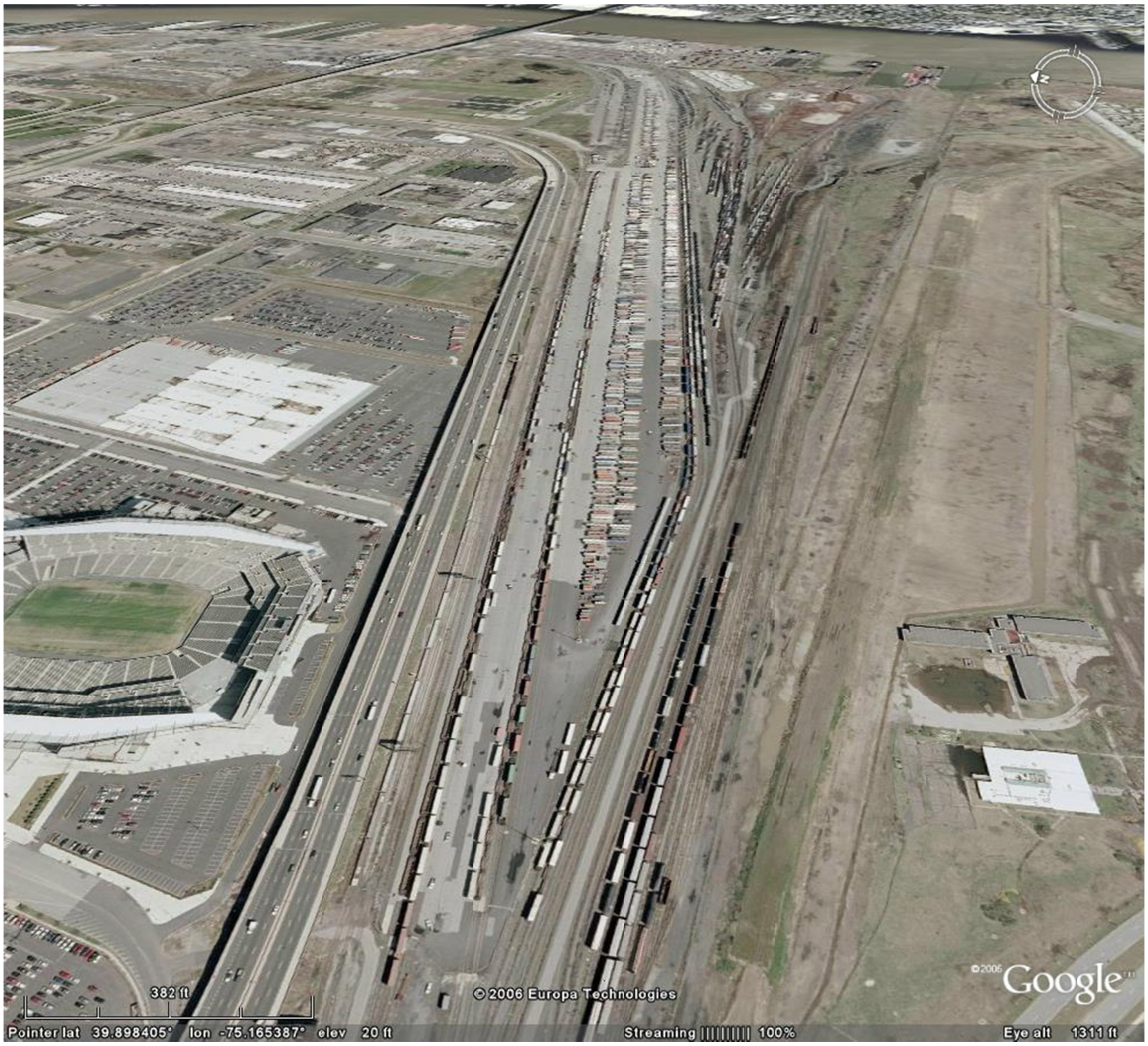

382 ft
© 2006 Europa Technologies
©2006 Google
Pointer lat 39.898405° lon -75.165387° elev 20 ft
Streaming |||||||| 100%
Eye alt 1311 ft

Figure 3-9. The Port of Philadelphia Rail Facility.

(Image source - Google Earth)

A typical train can consist of 100 rail cars or 200 to 300 containers. Containers are stacked on the rail cars: two (2) 40 foot containers are stacked on each other, one (1) 40 foot container can be stacked on two 20 foot containers, or one over-height container can ride solo.

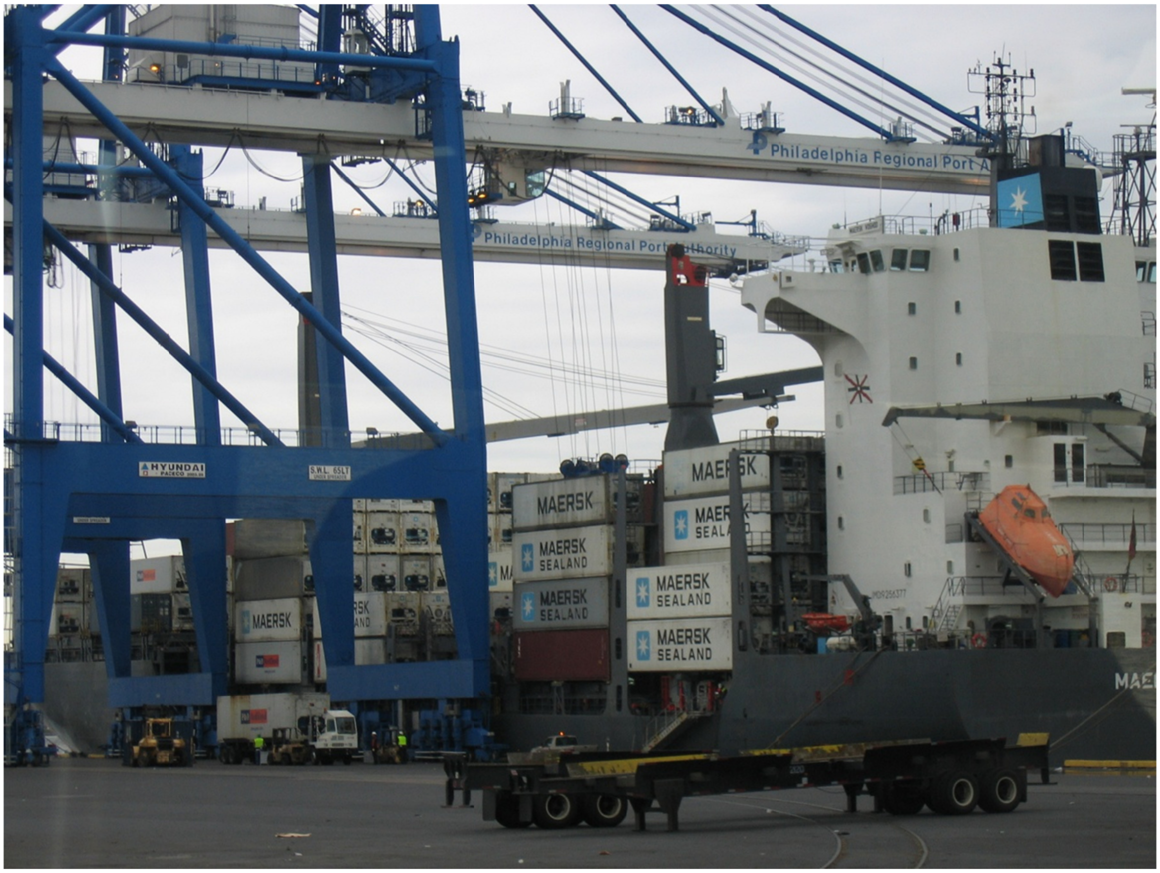


Figure 3-10. The Port of Philadelphia Cargo Unloading Operation.

The containers are off-loaded from the ships by way of a gantry crane. This is the typical operation for all container ports. The containers are loaded onto skates for movement aroung the port.

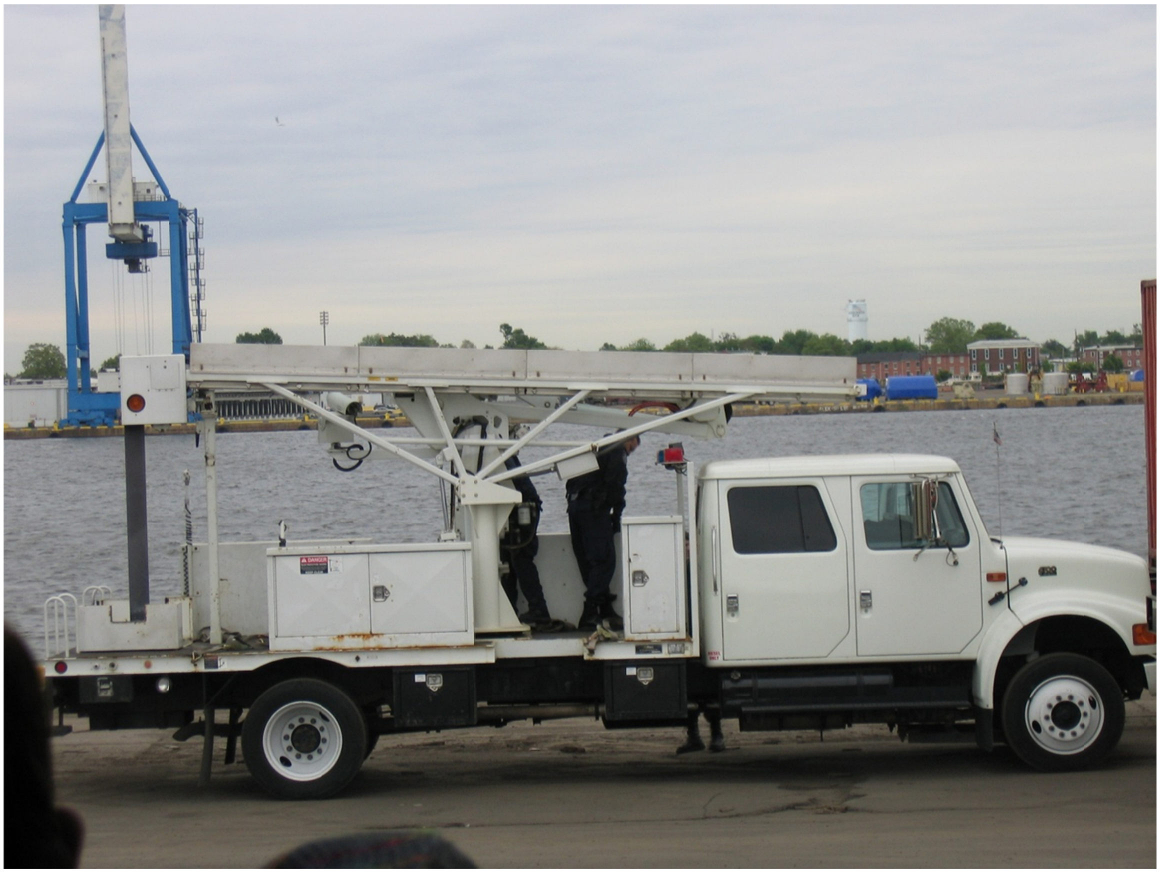


Figure 3-11. The Port of Philadelphia VACIS Gamma-Ray Truck.

At the Port of Philadelphia as well as dozens of U.S. seaports and border crossings, specially modified trucks with spidery metal arms are the newest high-tech weapon for U.S. customs inspectors in the war on terrorism.

The VACIS devices use gamma-ray imaging mounted at the end of the truck arms to allow human inspectors to check the contents inside the sealed steel containers. This helps to speed up cargo inspections, keeps the vital flow of commerce moving of anxiety.

3.1 Port of Catoosa Background

Background information is provided by the Port of Catoosa.

3.1.1 Port Location

The McClellan-Kerr Arkansas River Navigation System is a 440-mile waterway linking Oklahoma and the surrounding five-state area with ports on the nation's 25,000-mile 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 Tulsa Port of Catoosa, near Tulsa, Oklahoma, is located at the head of navigation for the System. The waterway travels 445 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 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 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.

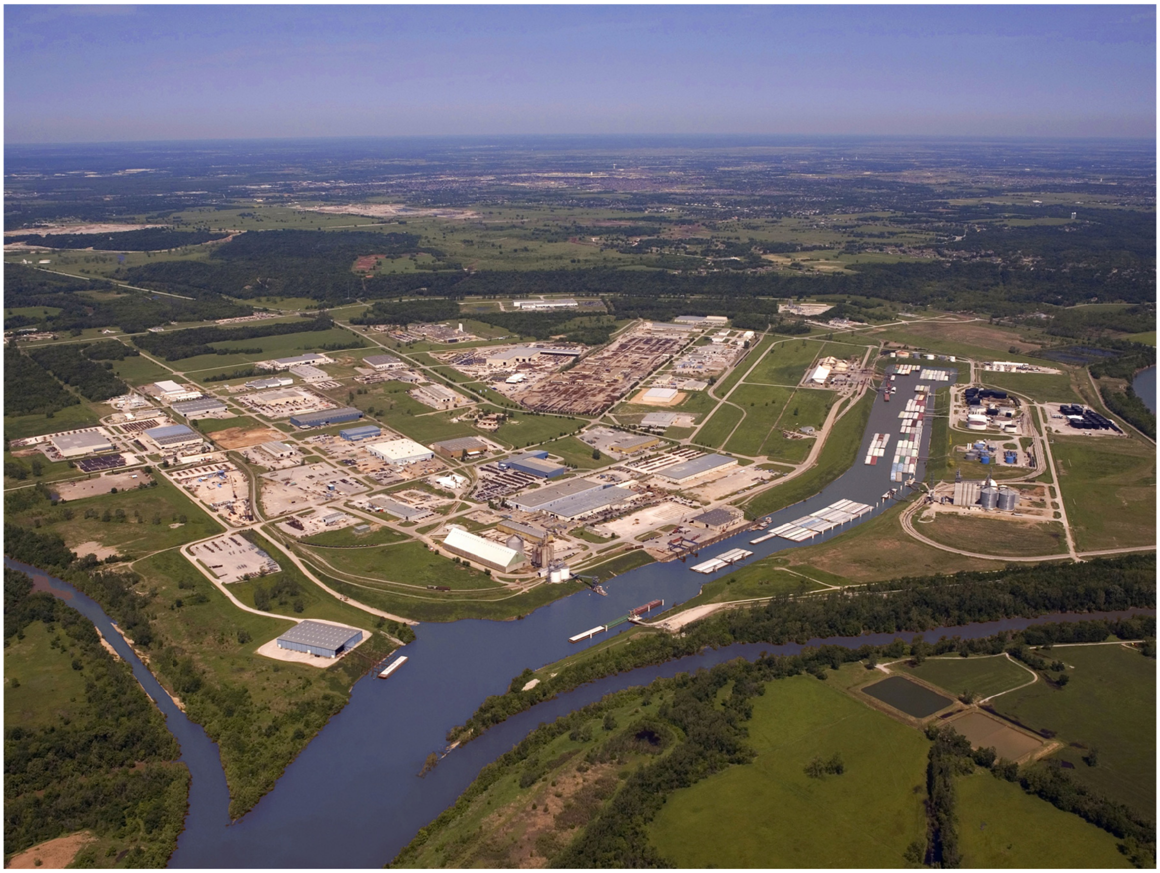


Figure 3-12. Aerial View of the Port of Catoosa.

(Image source - Tulsa Port of Catoosa)

3.1.2 Port Facilities

The Tulsa Port of Catoosa has five public terminal areas; each fully equipped and staffed to efficiently transfer inbound and outbound cargos between barges, trucks and rail cars. The assets of these terminals, with the exception of the liquid bulk facilities, are owned by the Tulsa Port of Catoosa but are maintained and operated by independent contractors that have lease agreements with the Port Authority. The liquid bulk companies are private and own their own facilities.

General Dry Cargo Dock

The general dry cargo dock primarily loads and unloads commodity iron and steel, project cargo and other breakbulk material. Operated by Tuloma Stevedoring, Inc., it is a public dock, 720 feet long, with a 230-foot wide concrete apron, equipped with an assortment of forklifts and cranes, including a 200-ton overhead traveling bridge crane.

Roll-on/Roll-off Low Water Wharf

The Roll-on/Roll-off wharf is a public dock operated by the Port Authority for transferring over-dimensional or over-weight project cargo such as giant processing equipment used in refineries. The wharf is 180 feet long with a 50-foot wide concrete

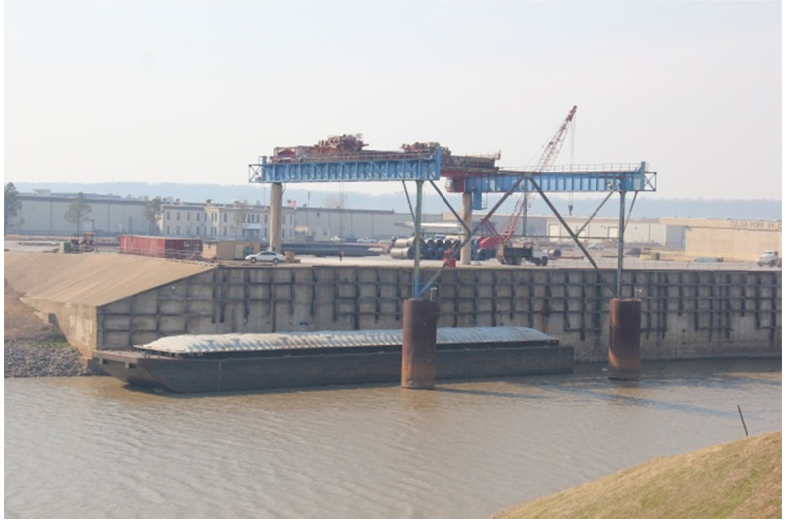


Figure 3-13. Overhead Travelling Bridge Crane.

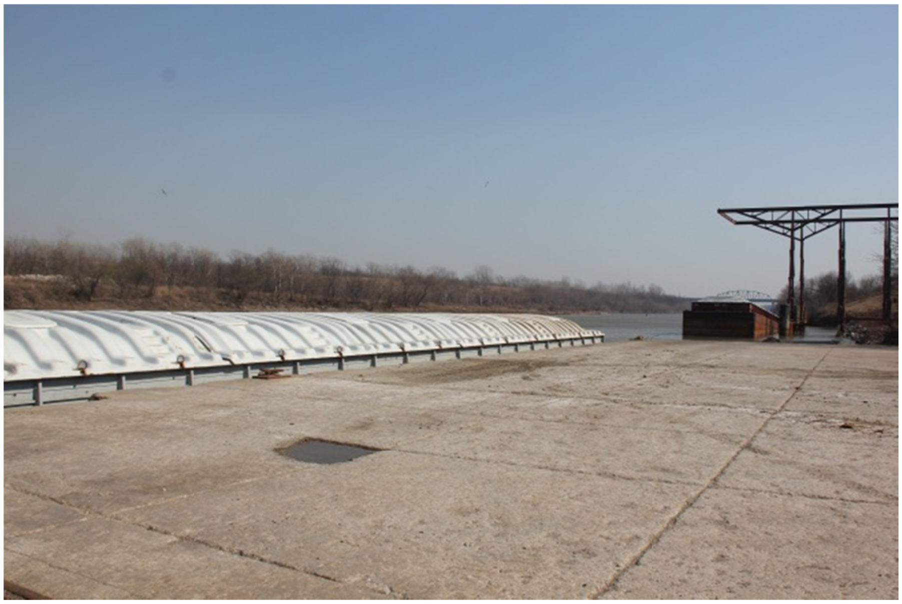


Figure 3-14. Roll-on/Roll-off Low Water Wharf.

apron and embedded railroad tracks. The dock is connected to a concrete road with a gentle 3.2 percent slope. Loads exceeding 600 tons can be driven directly onto to off of giant ocean-rated flat-deck barges using rail cars, trucks or wheeled transporters.

Dry Bulk Terminal

The Port's dry bulk terminal is a public terminal operated by Catoosa Fertilizer Co. A wide range of dry bulk commodities, from fertilizer to pig iron, can easily be transferred between modes of transportation. Inbound and outbound systems can load or unload up to 400 tons per hour. Covered storage is available for 80,000 tons of material and open storage for 50,000 tons. The terminal is equipped with two pedestal cranes and an outbound loading conveyance system. Unit train transfers are also possible.

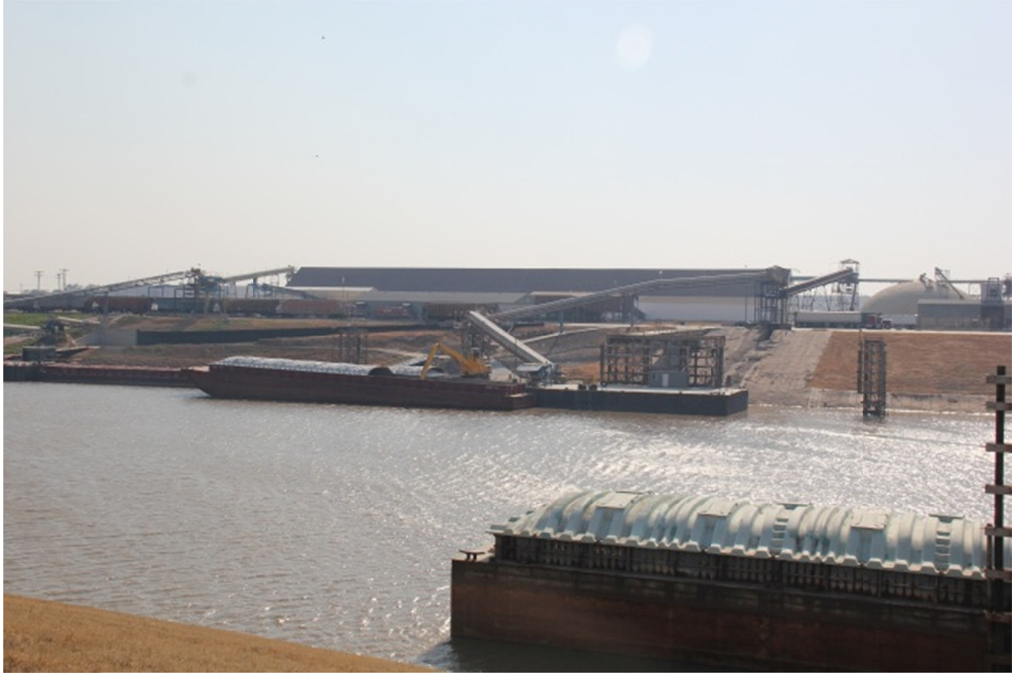


Figure 3-15. West Dry Bulk Terminal off-loading grain.

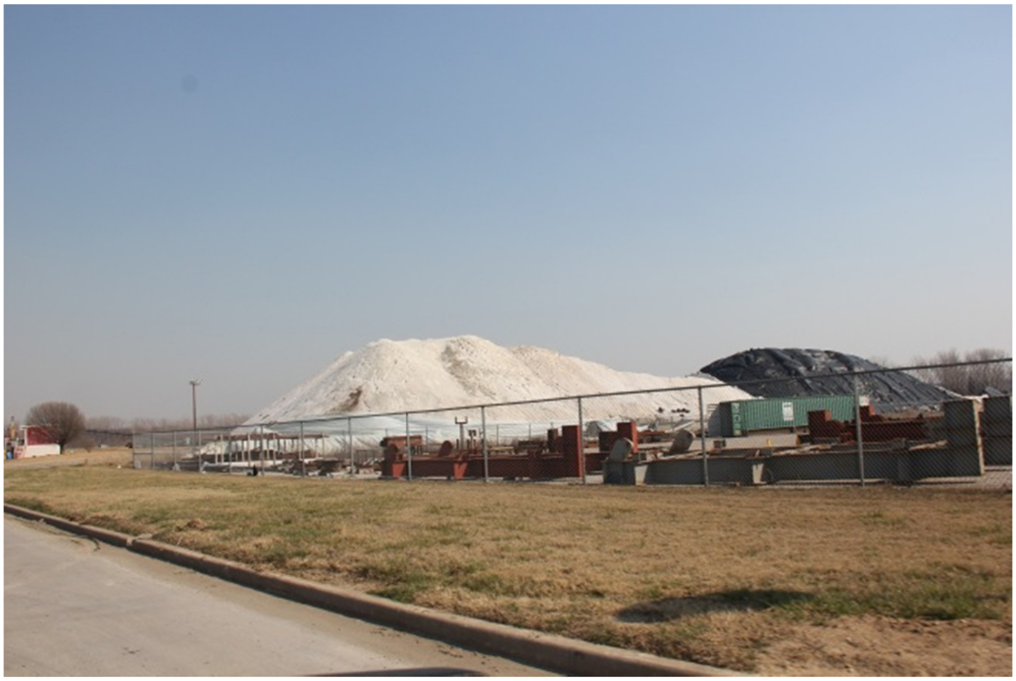


Figure 3-16. Uncovered Storage at the Port of Catoosa.

Grain Terminals

The Tulsa Port of Catoosa has two grain handling facilities – one public and one private. The public grain terminal is operated by Peavey Company, a division of ConAgra - the private terminal by DeBruce Grain, Inc. Facilities include outbound conveyance systems with 25,000-bushel-per-hour capacity, inbound unloading systems with a 30,000 bushel per hour capacity, grain samplers, dust control systems, and approximately 5.0 million bushel storage capacity. Grain grading is available on-site. The major product handled by these terminals is outbound hard red winter wheat, but inbound or outbound soybeans, oats, milo and millet can also be handled. Grain barges can be loaded in as little as 2.5 hours. These facilities will remain open 24 hours per day in peak season as necessary.

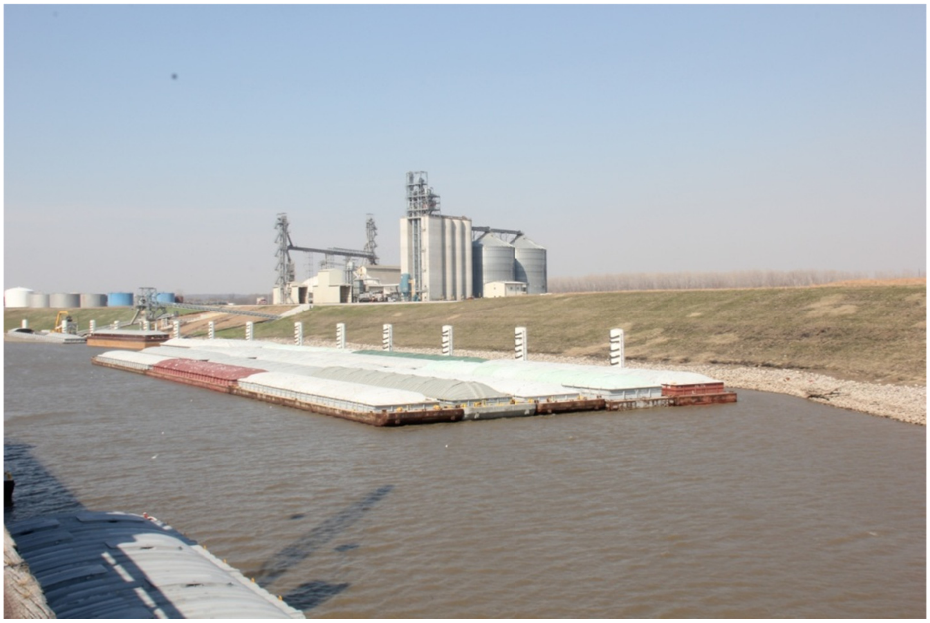


Figure 3-17. Grain Elevators at the Port of Catoosa.

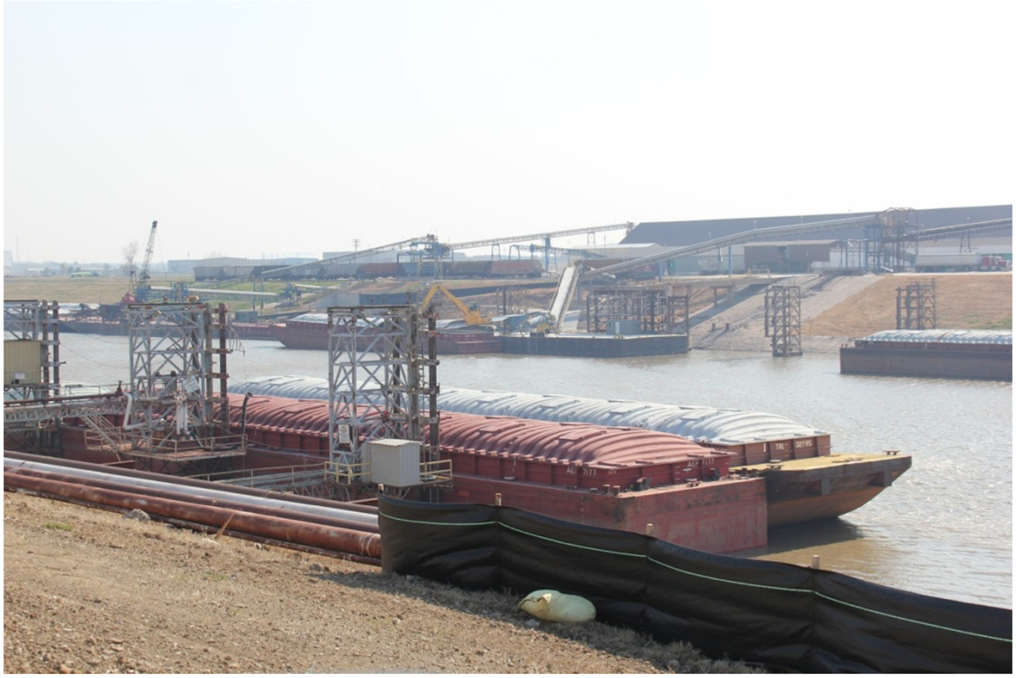


Figure 3-18. East Dry Bulk Terminal at the Port of Catoosa.

Bulk Liquids Terminal

Many types of bulk liquids, including chemicals, asphalt, refined petroleum products and molasses are transferred and stored at seven private terminals at the Port. These terminals should be contacted directly for information regarding the types of materials they handle and quotes for shipping, loading and unloading.

3.1.3 Port Shipping Methods

The Tulsa Port of Catoosa is an inland multi-modal shipping complex. Each day products are moved through the Port using barge, rail, and truck - often in combination.

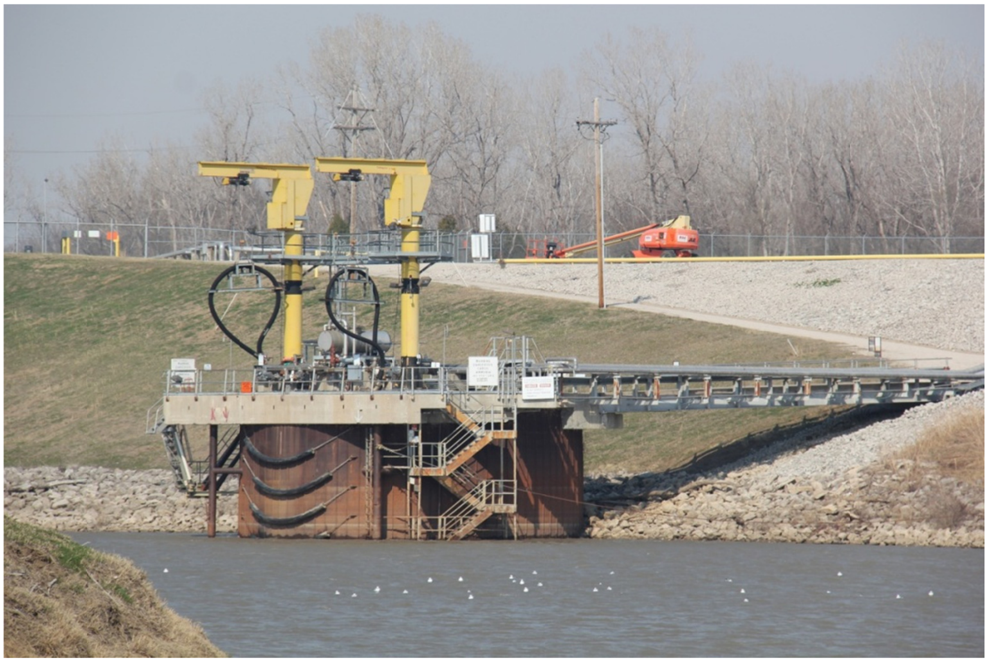


Figure 3-19. Bulk Liquids Terminal.

The Port's transportation assets include the waterfront docks and terminals and the 1.5-mile private channel on which they are located.

The Port owns two locomotives, serving the terminals and 20 private industry spurs on its 12-mile short-line system. It also owns two switch-boats, which move barges between the docks and the fleeting areas along the Port's channel. These services are performed by the Port's contract operators, the Port of Catoosa Railroad, and the Peavey Company.

Inter-port drayage of break-bulk cargo (especially steel) is offered by Tuloma Stevedoring, the Port's contract operator of the general dry cargo dock. With limited exceptions, all loading, unloading, and transfers occur on Port industry spur-tracks or at these docks with services performed by the terminal operators.

"Door-to-Door" arrangements for freight are contracted between shippers and third party service providers. While neither the Port Authority nor its terminal operators make such arrangements, both are glad to assist by connecting you with those who do.

In general, a shipper's choice of modes is determined by size (weight and or dimensions) and value of the shipment, as well as time requirements.

River Barges

For bulk and break-bulk cargo, barge shipping is best for shipments in excess of 1,500 short tons (30,000 cwt, the capacity of a standard hopper barge) or increments thereof. Both origin and destination points must be barge capable since multiple shifts between modes will erode savings. Freight arrangements are typically made through barge lines who provide the barges and contract with third parties for river towing. Transit times on the U.S. Inland waterway system average 100 miles per day.

Certain high-value fabricated pieces or "Project Cargo" are barge candidates as well. These are typically international shipments trans-loaded to or from ocean vessels at the Port of New Orleans or the Port of Houston. Such shipments are often restricted by weight or cubic dimension from moving on trucks or rail. The Port's Roll On/Roll Off ("RO-RO") Wharf can accept any such shipment. Freight arrangements for these are made by heavy-lift transport companies or project forwarders.

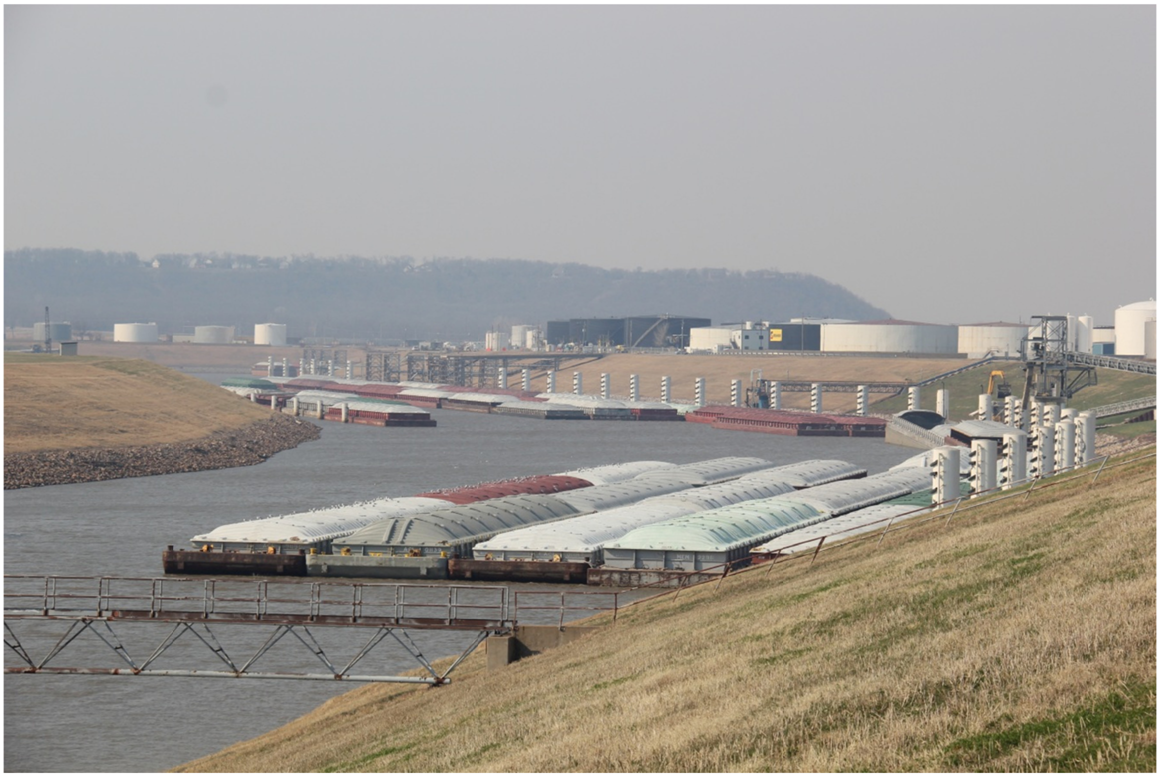


Figure 3-20. Bulk Barges at the Port of Catoosa.

Trucking

The Port is served by most of the nationwide contract carriers and averages over 450 trucks per day. Truck shipments are usually “next-day” requirements and average 20 short tons (400 cwt). Most truck shipments are to or from bulk storage at the Port’s terminals or for plants in the general industrial park. Located near the geographic center of the U.S., truck traffic can reach either coast in just two days.

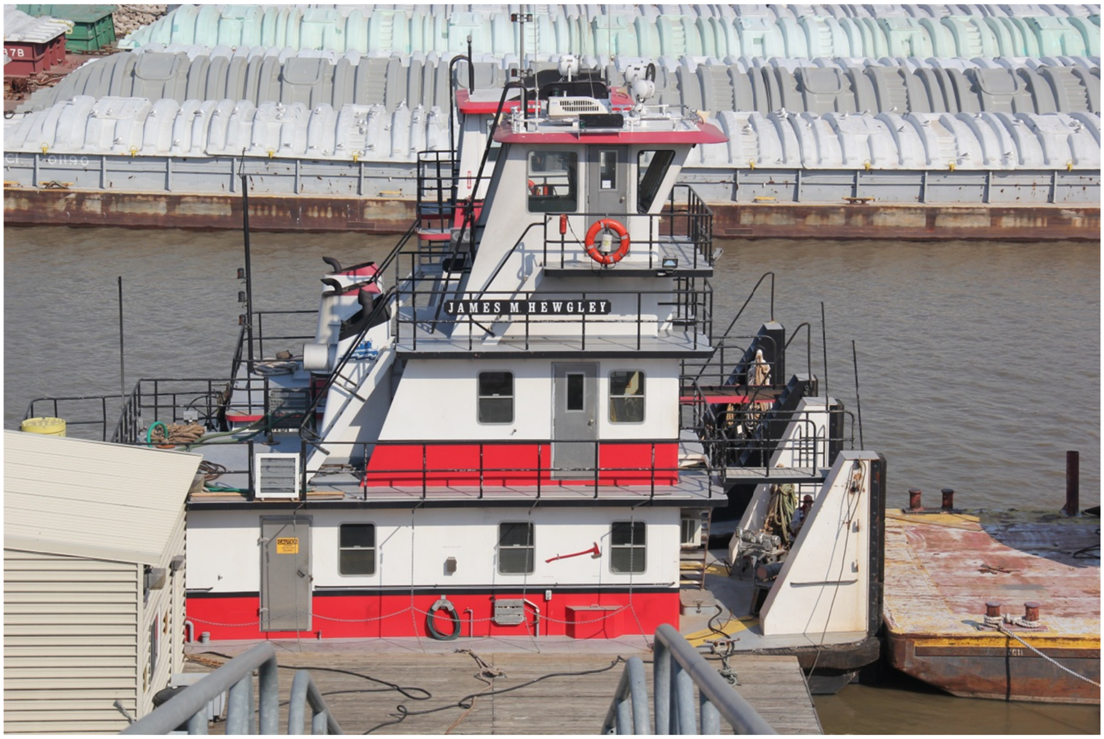


Figure 3-21. Prot of Catoosa Tug Boat – James M. Hewgley.

> James M. Hewgley was the Mayor of Tulsa, Oklahoma from 1966 to 1970, the Tulsa Port of Catoosa was constructed during his tenure as Mayor and the Port was inaugurated on June 5th, 1971 by President Richard M. Nixon.

Railroads

Rail shipping is ideal for most bulk and break-bulk cargo in average units of 100 short tons (2,000 cwt). Most of the national rail network is privately owned by the “Class I” operators. The Port is served by both of the remaining Western Class I Carriers, the BN-SF (direct) and the U.P. via a short-line switch on the South Kansas and Oklahoma

Railroad. The South Kansas and Oklahoma is a Class III with an extensive network in both Kansas and Oklahoma. Rail service is usually booked with the origin carrier who typically provides the cars. The Port is a scheduled service point for all three carriers. Rail transit times for most bulk and break-bulk cargo are roughly equal to barge within 750 miles and are days shorter beyond 1000 miles.

Airlines

Adding to the Tulsa Port of Catoosa's accessibility is the Tulsa International Airport. Just seven miles from the Port, this large, modern airport is served by major passenger carriers such as American, Continental, Delta and Southwest, and cargo carriers including FedEx, UPS and Airborne.

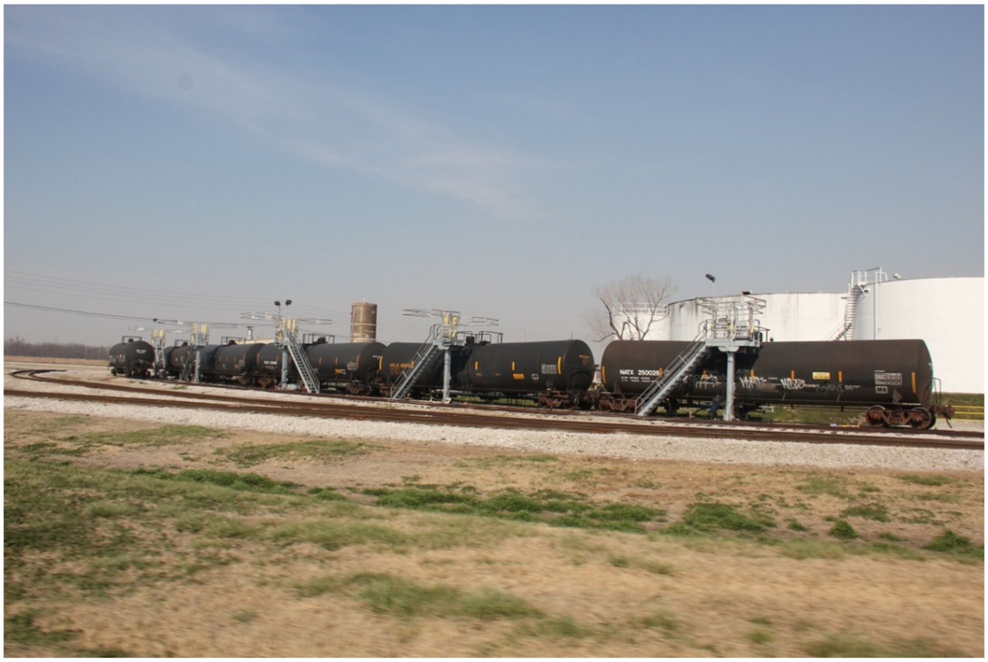


Figure 3-22. Asphalt Train Cars at the Port of Catoosa.

Containers

World-wide, containerized shipping is the wave of the future. A sealed container can be shipped around the world on a single bill of lading eliminating redundant documentation and pilferage during inspections. Current capacity for barge container shipping is 30 - forty foot containers. When the waterway is deepened to 12 feet, the capacity will increase 30 percent.

3.1.4 Foreign Trade Zone 53

The Tulsa Port of Catoosa is home to Foreign Trade Zone 53.

A Foreign Trade Zone (FTZ) is a secured site within the United States where foreign imports and domestic merchandise are considered to be outside U.S. Customs territory. Goods in the zone remain in international commerce as long as they are held within the zone or until they are exported.

The zone provides many financial and operating benefits for the user – particularly improved company cash flow. For instance, customs duties and taxes can be deferred on products or materials imported into the zone, or reduced by assembling components into final products within the zone. Duties and taxes may also be substantially reduced or avoided by inspecting and destroying substandard materials or defective merchandise in the zone. Bulk shipments may be purchased economically, brought into the zone and repackaged before being marketing in the U.S.

3.1.5 Bonded Warehouse

In addition to the FTZ, imported goods may be stored in one of the Port's bonded warehouses which are owned and operated by Miles Shipping Co.

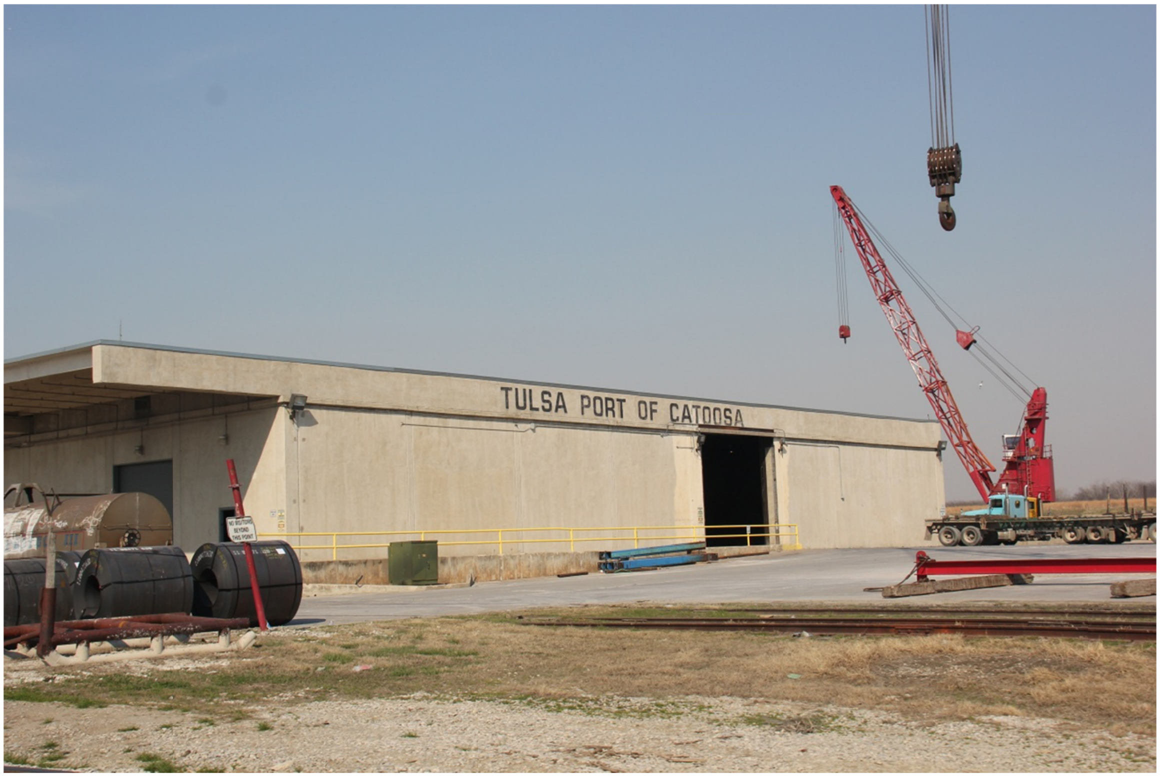


Figure 3-23. Warehouse at the Port of Catoosa.

3.2 Demonstration Project Objectives

The objective of the demonstration project at the Tulsa Port of Catoosa is to provide a test bed for intermodal freight movement tracking, and security. By creating a real environment for freight movement and storage, sensors, robots, networks, and vehicles can be operated, evaluated, and stressed to evaluate their application to the overall project.

3.3 Demonstration Project Activities

On the Port of Catoosa, an area was designated for container storage. Entrance and exit from this area was controlled and monitored for sensor and security evaluation.

A wireless network was deployed on the port. Network nodes enabling 802.11a/b/g were installed at four locations to provide maximum port coverage while ensuring that a variety of activities can be monitored. See Figure 3-24 for network node locations.

Video surveillance was tested using a variety of cameras. Mobile cameras on ground surveillance vehicles, aerial cameras on aerial surveillance vehicles, and fixed cameras were tested. Video was encoded and provided via the wireless network to the central server.

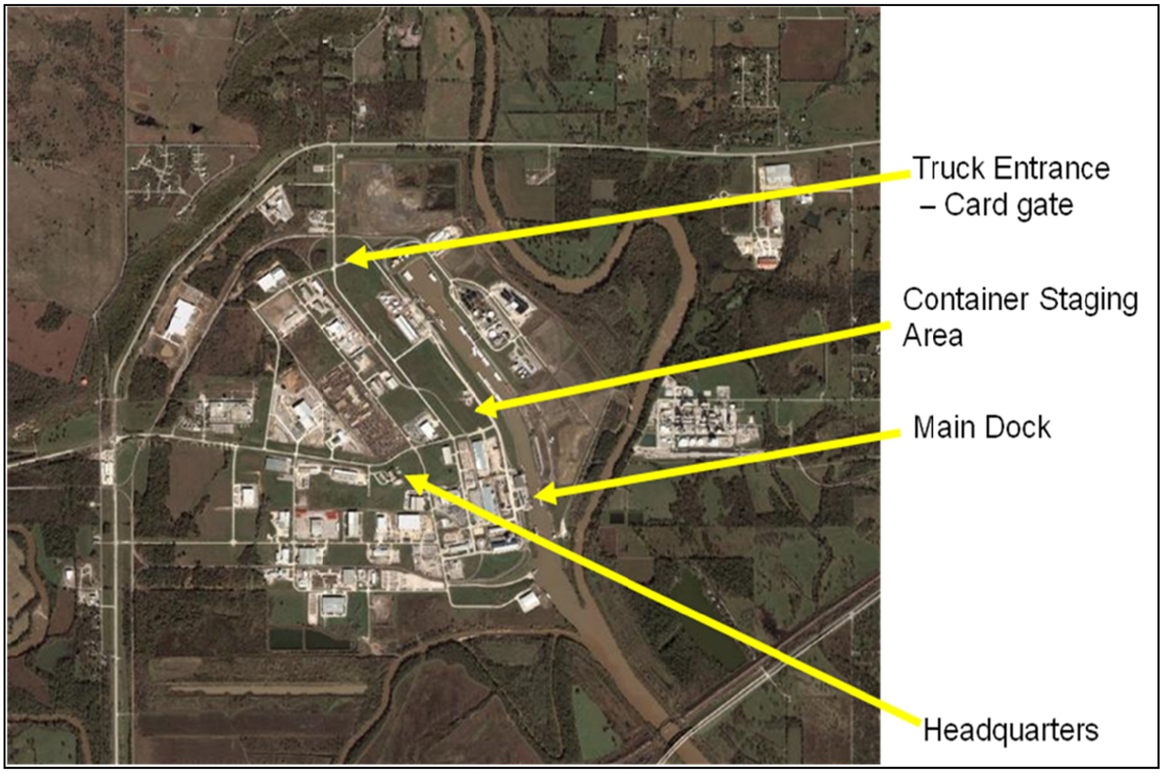


Figure 3-24. Network Node locations at the Port of Catoosa.

(Image source - Google Earth)

Sensors were deployed at the entrance points to the container area to track freight movement into and out of the area. Sensors were also be deployed on the containers. Some of the sensor monitoring parameters were: temperature, humidity, acceleration/pressure, vibration, and light.

Radio Frequency Identification (RFID) readers were used as appropriate to read RFID tags and E-Seals when sensors are not practical or warranted. Both active and passive RFID technologies were used.

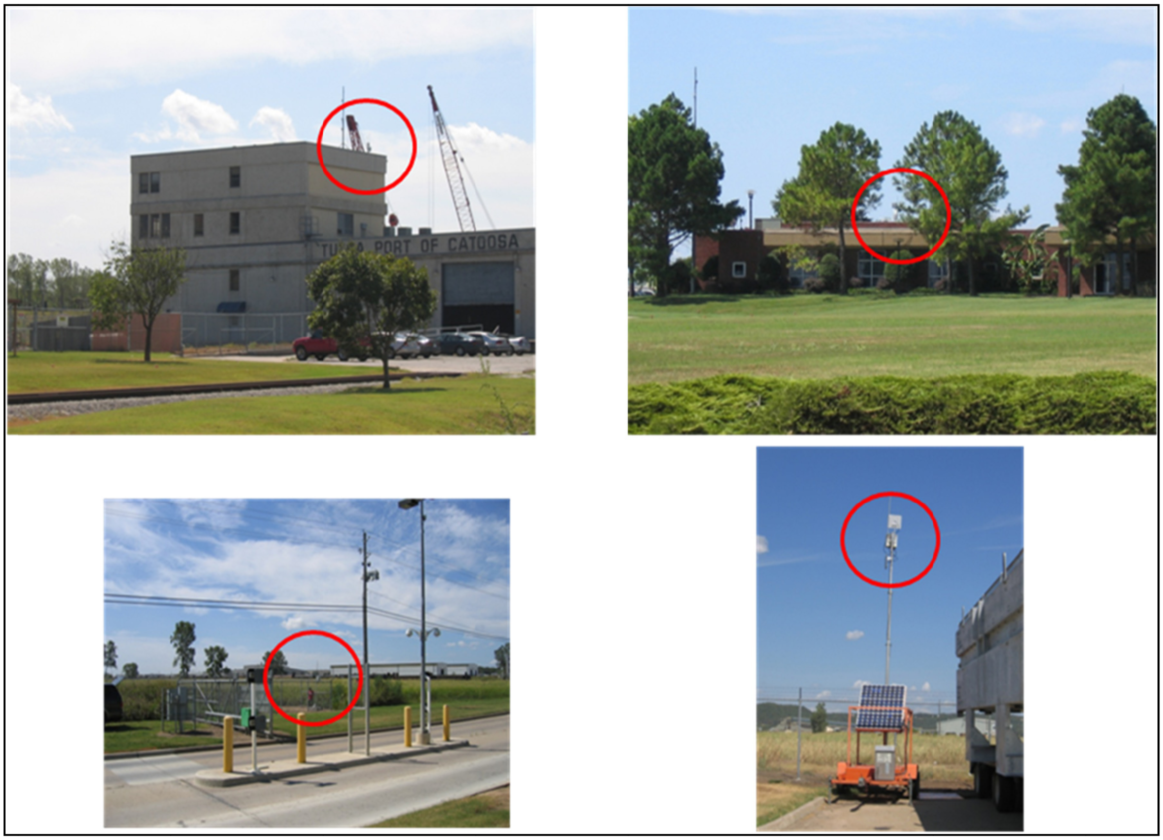


Figure 3-25. Close up of Network Node locations at the Port of Catoosa

It was desired to test gamma detectors to detect containers containing radiation threats but will require further study.

The ground surveillance vehicle were used to interrogate the sensors and RFID devices while following a set pattern. The path was marked with stakes containing RFID tags to provide location updates to the central server. Other technologies were tested and characterized as part of the test bed. These other technologies included GPS and active

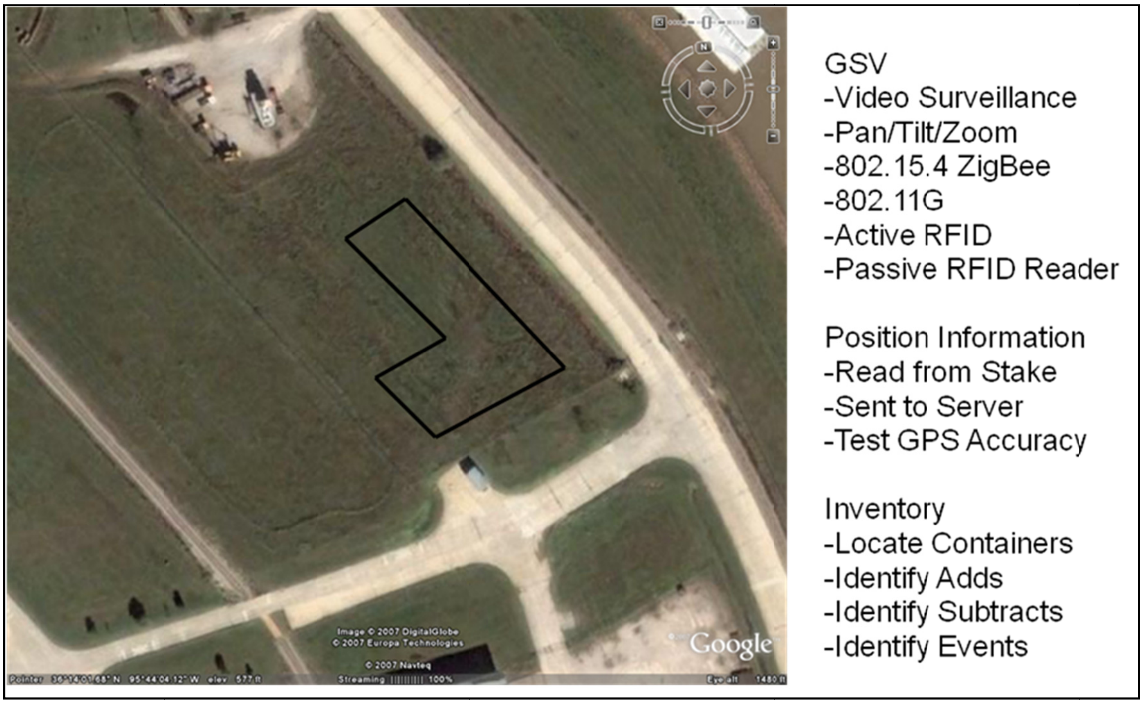


Image © 2007 DigitalGlobe
© 2007 Europa Technologies
© 2007 Navteq
Google
Pointer 36°14'01.68" N 95°44'04.12" W elev 577 ft
Streaming |||||||||| 100%
Eye alt 1480 ft

GSV
-Video Surveillance
-Pan/Tilt/Zoom
-802.15.4 ZigBee
-802.11G
-Active RFID
-Passive RFID Reader

Position Information
-Read from Stake
-Sent to Server
-Test GPS Accuracy

Inventory
-Locate Containers
-Identify Adds
-Identify Subtracts
-Identify Events

Figure 3-26. Proposed Ground Surveillance Vehicle Track and Capabilities.

(Image source - Google Earth)

RFID for real-time locating. See Figure 3-26 for Ground Surveillance Vehicle track and capabilities. The ground surveillance vehicle was employed with pan/tilt/zoom video and transmitted the video over the wireless network to the central server.

The ground surveillance vehicle also employed 802.15.4, 802.11g, and active and passive RFID capabilities for sensor interrogation. The ground surveillance vehicle was remotely controlled and capable of running autonomously around the fixed course.

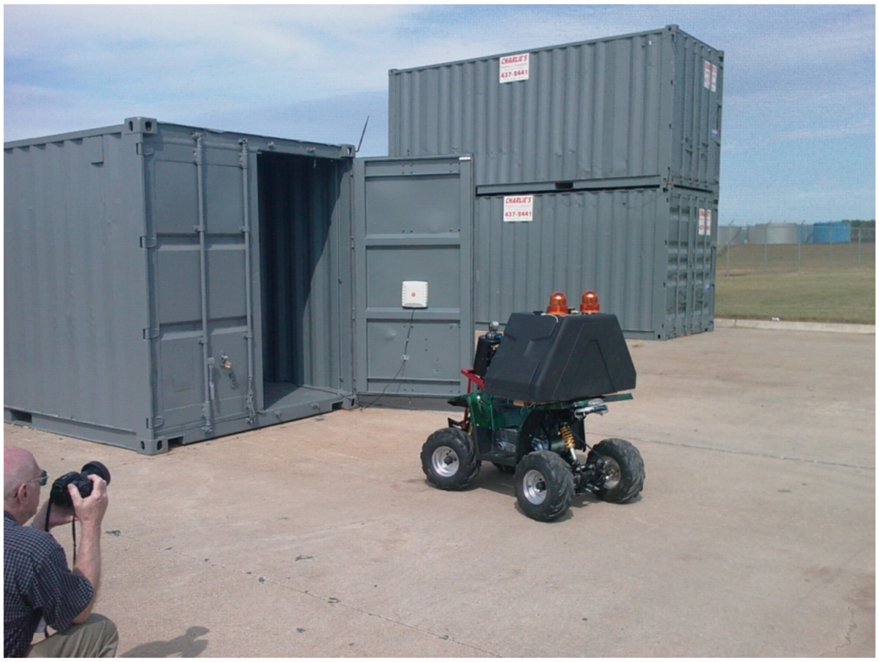


Figure 3-27. The Ground Surveillance Vehicle developed by Dr. Commuri and his team interrogating a container.

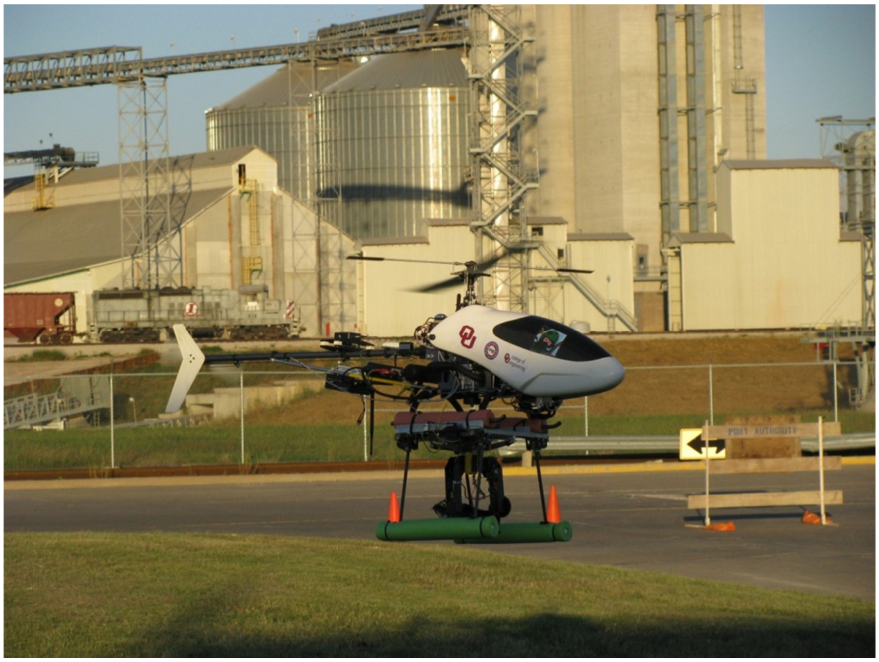


Figure 3-28. The Aerial Surveillance Vehicle hovering at the Port Of Catoosa.

Container presence was detected by the ground surveillance vehicle. Container information was sent over the wireless network to the central server.

The aerial surveillance vehicle was used for aerial video surveillance. Initial flight paths were fixed and autonomously flown. Further study will be required for autonomous flight plan redirection due to event notification from the ground surveillance vehicle or other event input. See Figure 3-29 for Aerial Surveillance Vehicle Locations. See Figure 3-30 for Aerial Surveillance Vehicle proposed flight path.

Aerial video surveillance pan/tilt/zoom camera commands were initially manual. Further study will be required for autonomous camera steering commands due to event notification from the ground surveillance vehicle or other event input.

The container area entrance was monitored using a variety of sensors to detect movement into and out of the area. Direction of movement and container information was sent over the wireless network to the central server.

The central server was the source of inventory information. Container ID, sensor data, location, and event information was stored on the central server.

Containers moving into and out of the container area require preclearance prior to movement. Containers moving without preclearance were flagged as events.

The central server maintained location information on the ground surveillance vehicle.

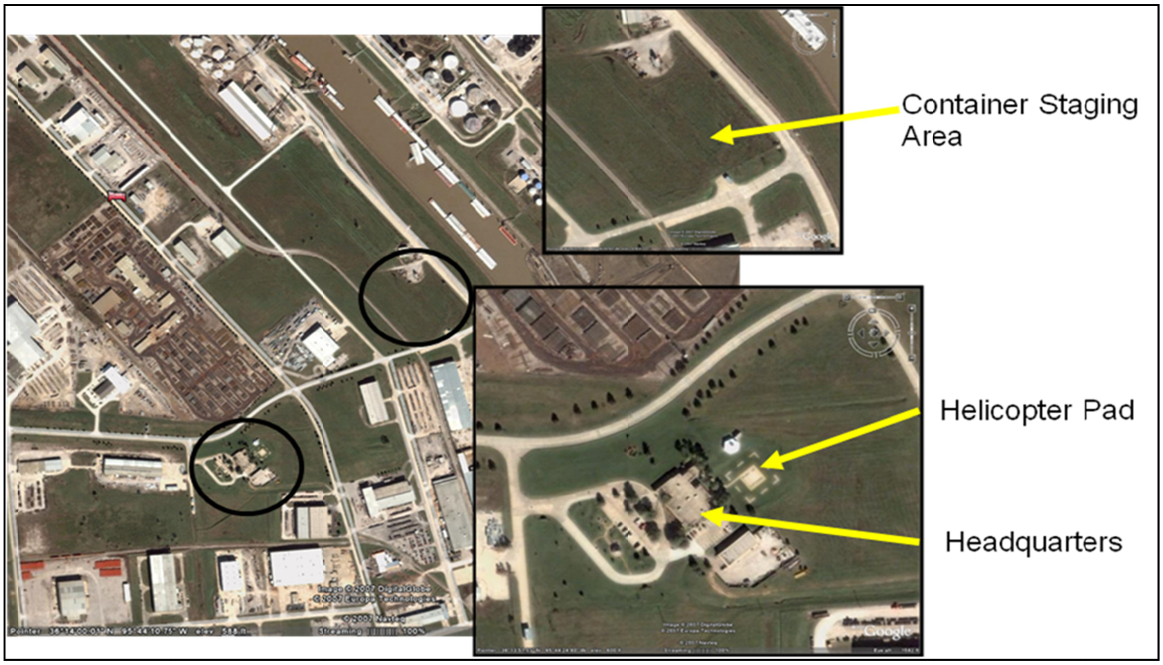
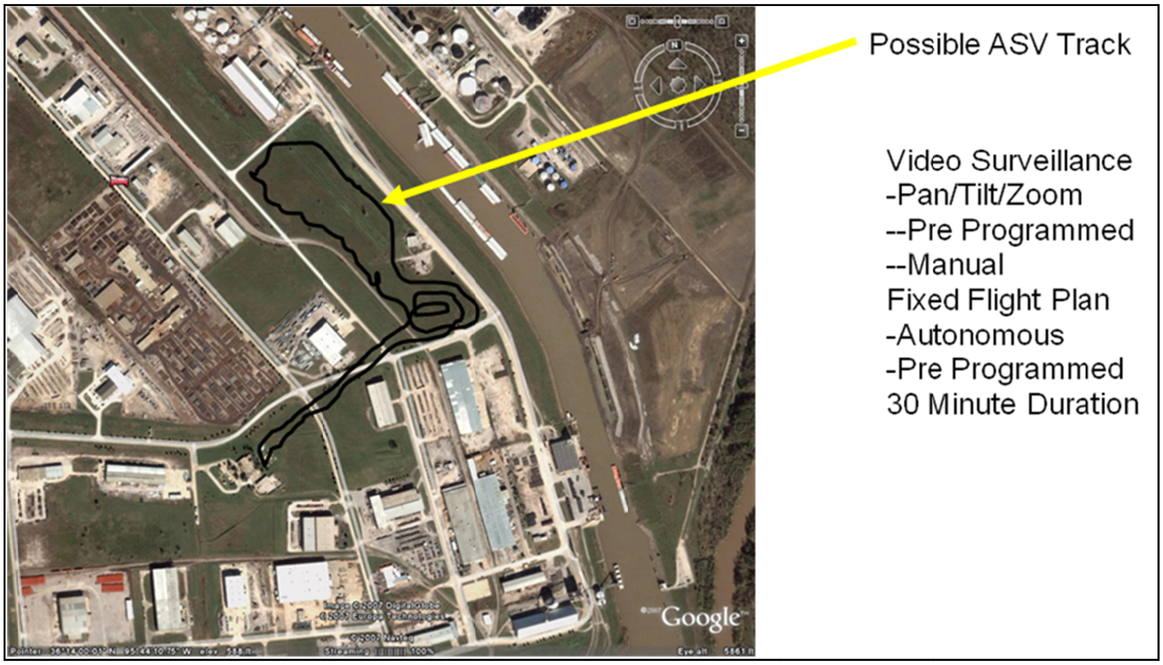


Figure 3-29. Aerial Surveillance Vehicle Locations.



Video Surveillance
-Pan/Tilt/Zoom
--Pre Programmed
--Manual
Fixed Flight Plan
-Autonomous
-Pre Programmed
30 Minute Duration

Figure 3-30. Aerial Surveillance Vehicle proposed flight path.

The central server identified events when the ground surveillance vehicle passed a location and does not report container status when a container has been inventoried in that location.

The central server identified events when sensor data or RFID data indicated tampering or out of tolerance conditions.

3.4 Container Instrumentation Activities:

3.4.1 Planning:

For demonstration, the planned deployment of four sensor base modules at the port of Catoosa occurred with the sensor systems that were developed by Dr. Tull and his group and sensors and software developed by Dr. Radhakrishnan and his group. Two of the sensors modules were equipped with cargo condition sensors.

Sensors:

Containers were equipped with both security and cargo integrity sensors. These sensors included temperature, humidity, light and acceleration.

The development was based on the use of Crossbow's TelosB and MicaZ development boards. These boards utilize global unlicensed ISM radio band of 2.4 GHz and the on board transceiver complies with IEEE 802.15.4 and ZigBee standards.

Readers:

The demonstration used three sensor readers. The demonstration deployed two readers to simulate port entrance and exit and one-sensor reader on the ground surveillance robot. Two readers at each exit and entrance were required to determine the direction of transportation.

Network:

The sensor network is a heterogeneous network that was comprised of ISO 18185 compliant 433 MHz and/or 2.4 GHz bands, and IEEE 802.15.4 compliant unlicensed 2.4 GHz ISM band.

At the reader end, both of these networks utilized a bridge to handover sensor data to the 802.11 b/g TCP/IP wireless network. An 802.11 wireless network was already being deployed as a part of this demonstration and that was be utilized to transport the seal and sensor data to the server.

Chapter 4 - Port of Catoosa Security Video Project

There was a potential funding opportunity for the Port of Catoosa to pursue funding from the Infrastructure Protection: Port Security Grant Program (PSGP), because of its status as a Tier III port, and current work with the ICFS program. Because of this opportunity, a video surveillance project that would have provided coverage of the entire Port of Catoosa was designed, however, funding was not received.

This project was to develop a proposal to equip the entire Port of Catoosa facility with real-time video feeds of the port, recording timed snapshots to a central video server, and allow efficient search capability for video retrieval.

Based on current plans for the demonstration project and considering long term plans for the port facility (Figure 4-1) an engineering estimate was accomplished. Figure 4-2 shows the proposed layout for the wireless mesh network based on the equipment that was also proposed for the demonstration project.

Figure 4-3 shows the approximate wireless network coverage of the IEEE-802.11A links. This is based on an engineering judgment of 50% RF signal coverage, allowing for obstructions and other interference from existing systems. A full coverage determination would require Signal Strength measurements and was not accomplished due to time and cost considerations.

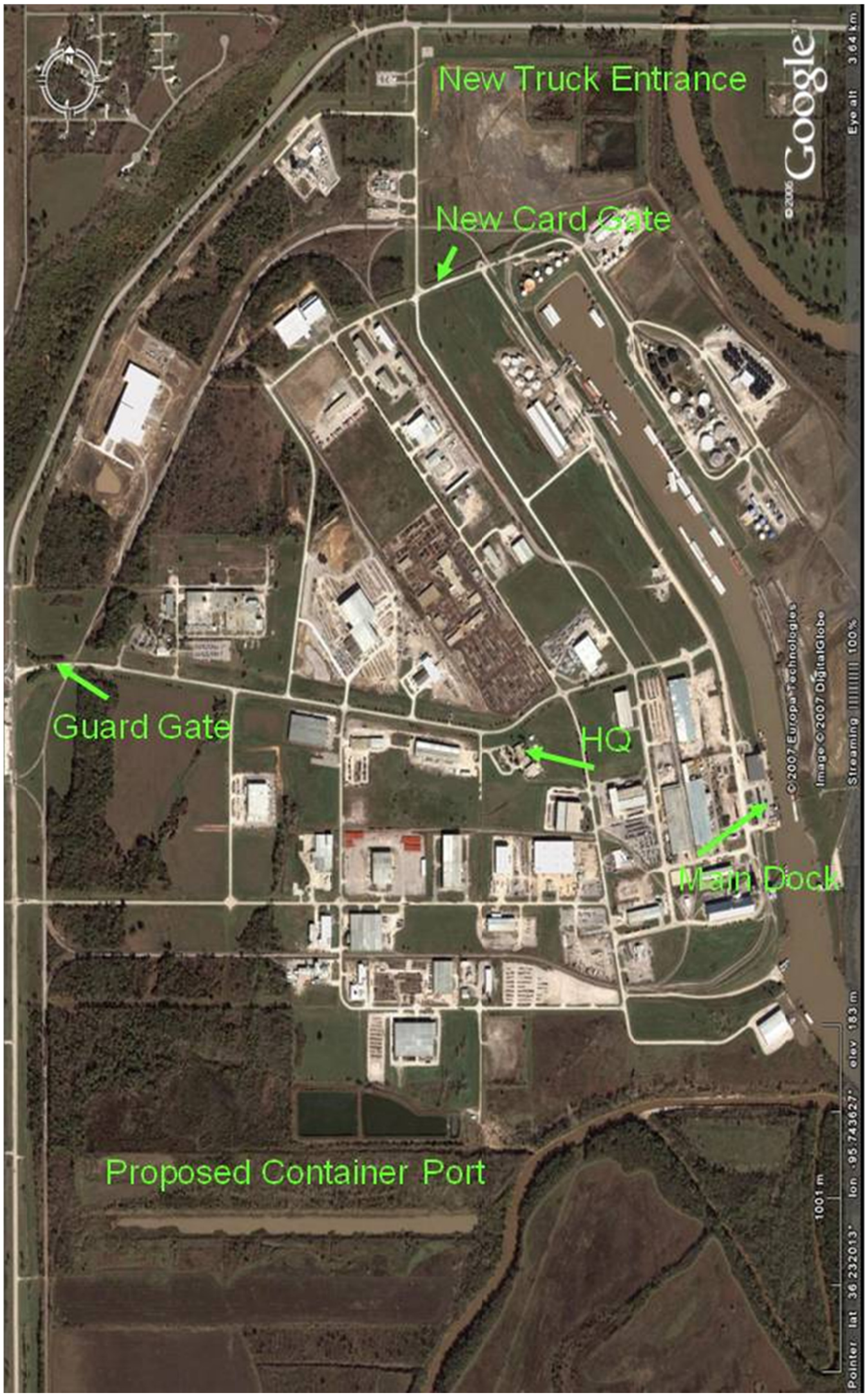


Figure 4-1. Satellite Image of the Port of Catoosa.

(Image source - Google Earth)

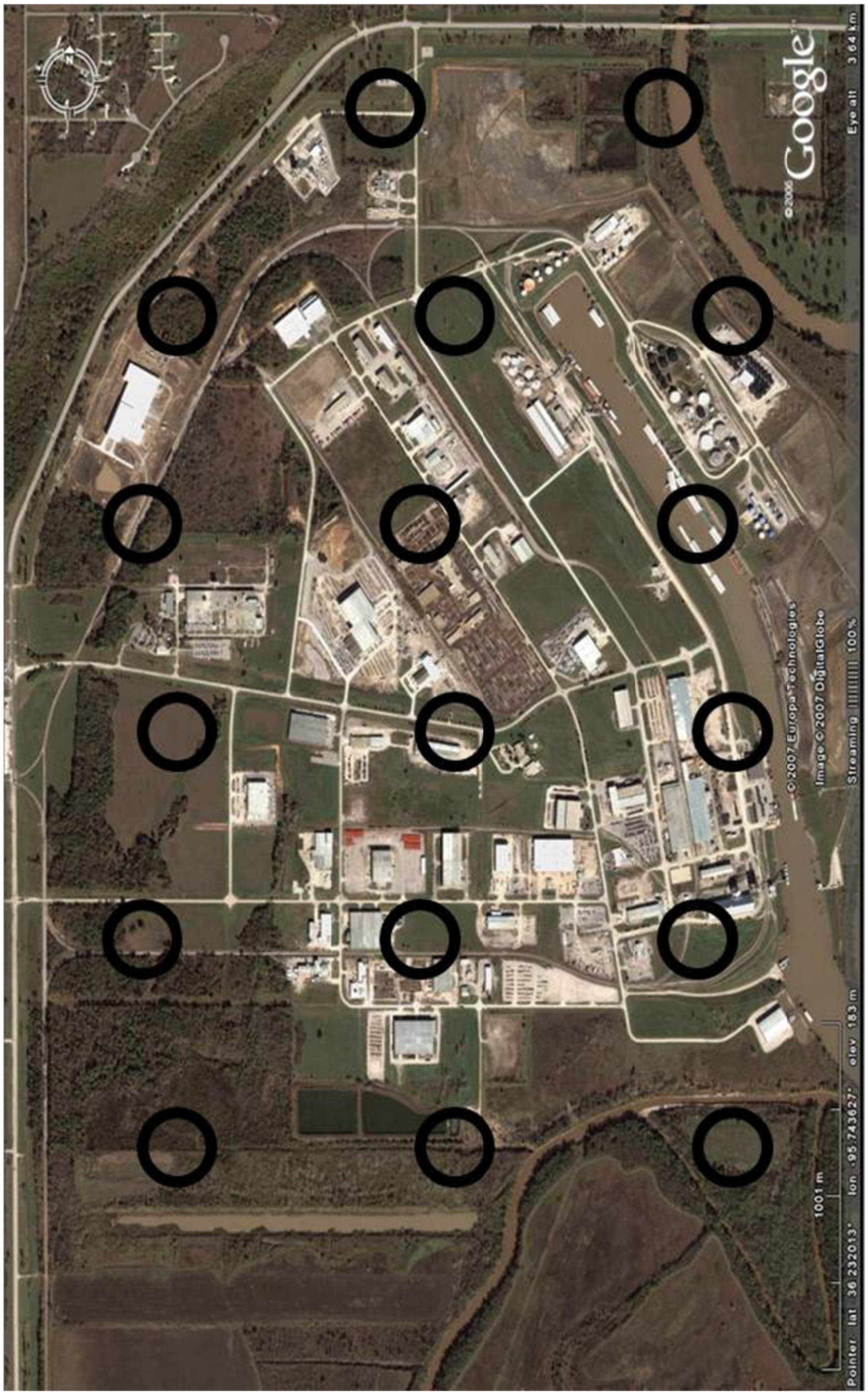

©2008 Google
Eye alt 3.64 km
©2007 Europa Technologies
Image © 2007 DigitalGlobe
Streaming |||||||||| 100%
1001 m
Pointer lat 36.232013° lon -95.743627° elev 183 m

Figure 4-2. Proposed Network Node Locations.

(Image source - Google Earth)

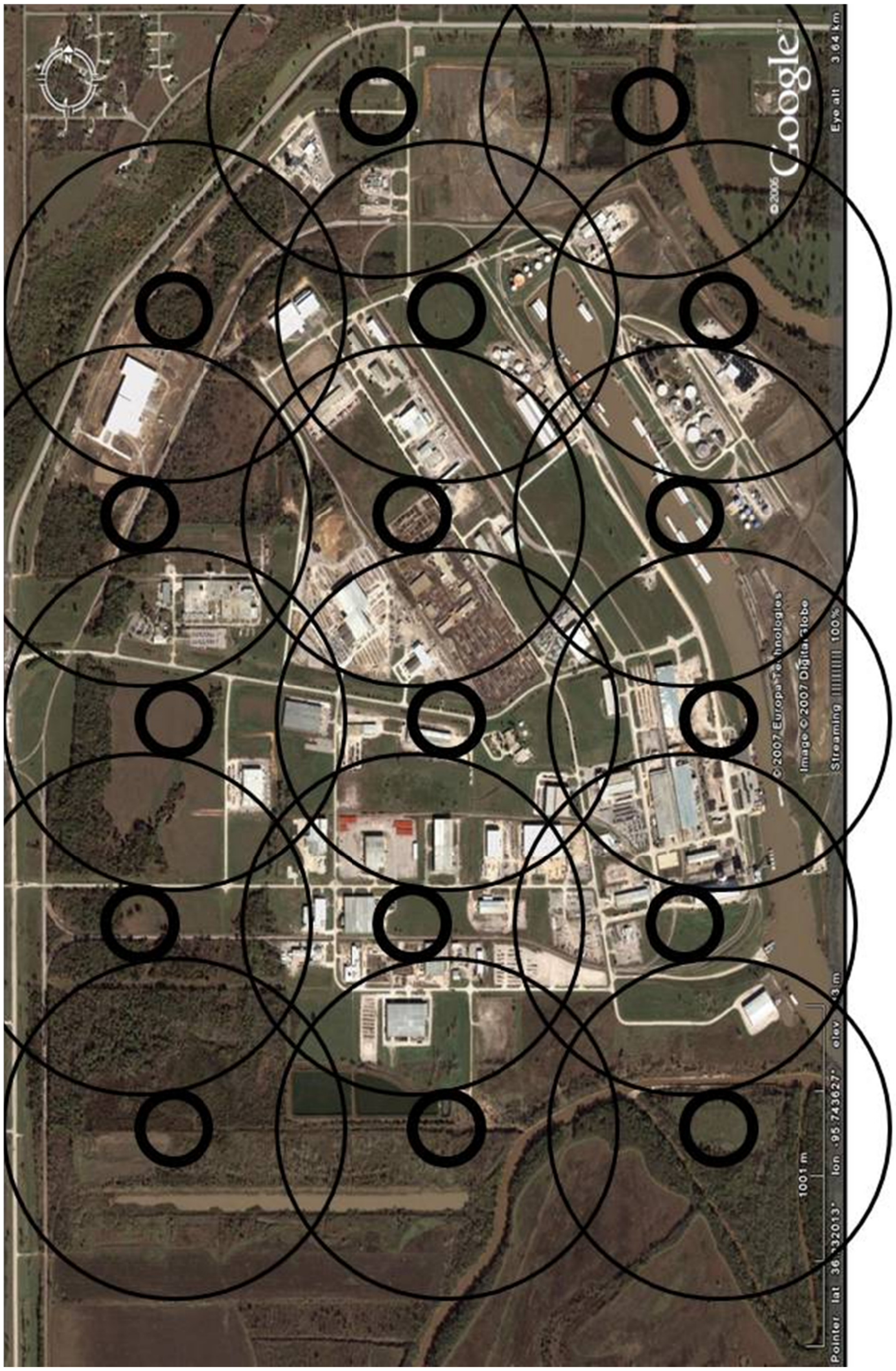

©2006 Google
Eye alt 3.64 km
© 2007 Europa Technologies
Image © 2007 DigitalGlobe
Streaming ||||||||| 100%
1001 m
Pointer lat 36.32013° lon -95.743627° elev 3 m

Figure 4-3. Projected Network Coverage Area

(Image source - Google Earth)

Figure 4-4 shows the approximate video coverage at the Port of Catoosa using standard AXIS IP web cameras with the standard 3.5mm lens. This project shows that video surveillance and recording of the entire port and surrounding areas can be accomplished with off-the-shelf cameras and network equipment as proposed in the demonstration project.

Final camera locations would be determined with a combination of the use of the well studied “art gallery problem” also known as the “museum problem” which is a visibility problem in computational geometry. In the computational geometry version of the problem the layout of the art gallery is represented by a simple polygon and each guard (camera) is represented by a point in the polygon. The expected result is typically [n/3] where n is the number of vertices of the polygon [19]. However this solution assumes that the cameras can see 360 degrees and have infinite range. Therefore, network node signal strength as well as camera angle and vision distance would also be necessary.

Table 4-1 is a cost estimate for this project. The $50K for utilities is an estimate from the electric company to install 20 service poles for the camera and network installations.

The estimated cost of $387.5K represents a small portion of the cost associated with a contractor developing a proprietary system of hardware and software without the future possibility of expansion or enhancement. For example, this type of cost comparison has been studied for the ITS deployment in the State of Oklahoma [5].

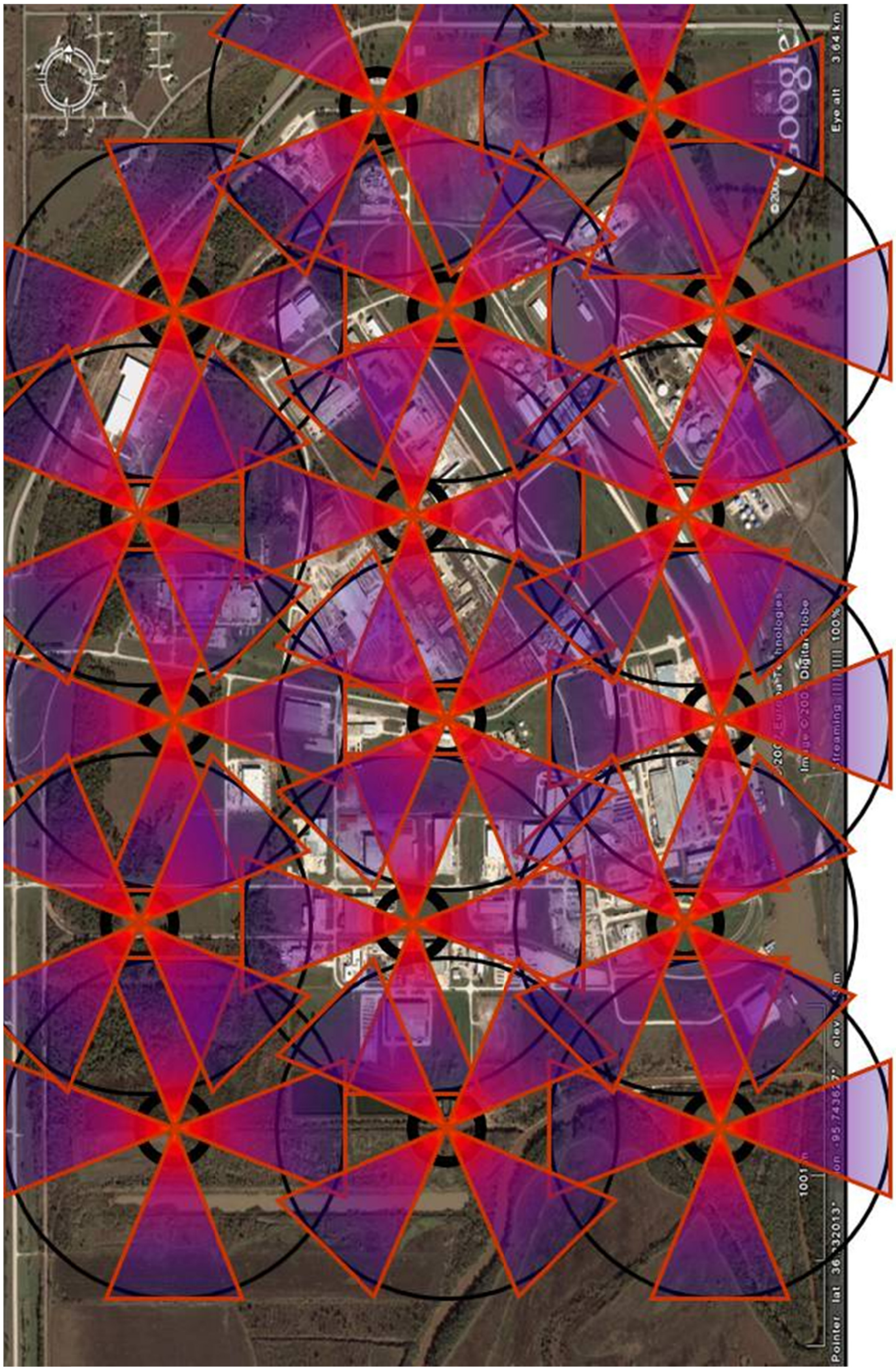

Google
Eye alt 3.64 km
©2008 Europa Technologies
Image ©2008 DigitalGlobe
Streaming 100%
Pointer lat 36.32013° lon -95.743627° elev
1001 m

Figure 4-4. Projected Camera Coverage Area

Table 4-1. Cost Estimate for the Port Video Project

20	Network Nodes	$100K
80	IP Network Cameras	$100K
20	Utility Service Poles	$50K
1	DVR w/computer and storage	$25K
	Installation	$75K
Sub-total		$350K
	IDC	$37.5K
Total		**$387.5K**

Chapter 5 - ICFS Project Phase II

The main focus of Phase II of the Intermodal Containerized Freight Security project was to provide a demonstration of several technologies that could be used to enhance port security. This research demonstrated that off the shelf technology could be used, specifically with the use of aerial surveillance, to augment foot patrols with an eye-in-the-sky, thus greatly enhancing their surveillance capabilities.

5.1 - Demonstration Project

This demonstration was designed to show the use of available off-the-shelf technology to augment security measures at a port facility. This research demonstrated the use of a semi-autonomous aerial surveillance vehicle equipped with a high-definition video camcorder and wireless video downlink to provide a birds-eye view of the port facility to security control center and security patrols on the ground.

5.1.1 - Tulsa Port of Catoosa

The Tulsa Port of Catoosa shown in Figure 5-2, near Tulsa, Oklahoma is located on the McClellan-Kerr Arkansas River Navigation System. This system is a 440-mile waterway linking Oklahoma and the surrounding five-state area with ports on the nation's 25,000-mile 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 445 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 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 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.

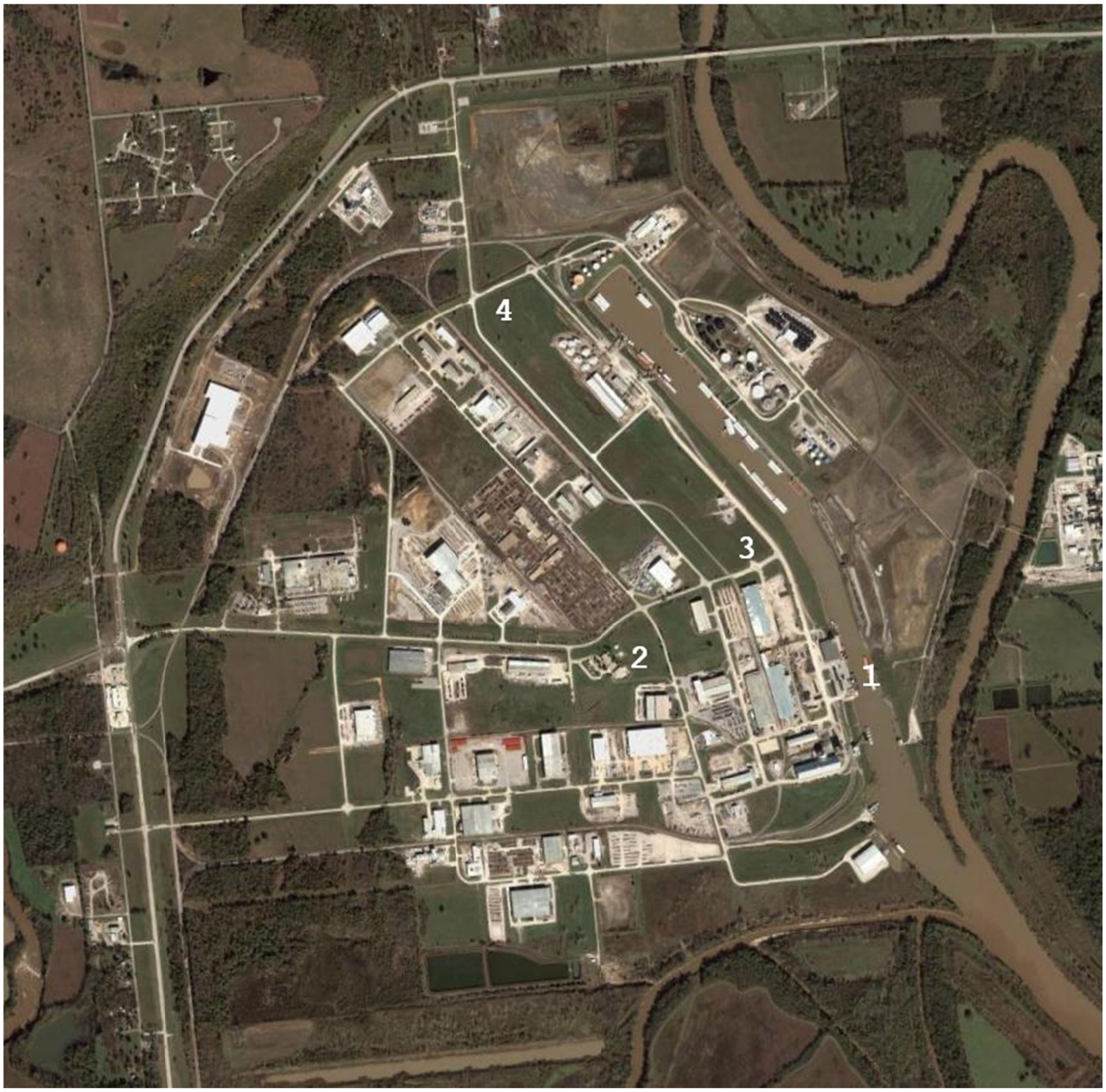


Figure 5-1. Port of Catoosa.

(Source of image – Google Earth)

Location 1 is the dock area for ship loading and unloading, location 2 is the Port Headquarters Building and Helipad, location 3 is the Container Storage Yard Demonstration Area, and location 4 is the Card Gate for truck entry and exit. All four locations are equipped with a wireless mesh network for data and video demonstrations

5.1.2 - The aerial surveillance vehicle

The ASV platform shown in Figure 5-2, is an Express G from Neural-Robotics, Inc., and is based on a gas-powered Vario Benzin Trainer helicopter. The ASV is capable of carrying ten pounds of payload for 60 minutes. The operator transmitter/controller is a Futaba 9C Super operating at 72 MHz. The ASV includes basic avionics components consisting of a PC/104 computer running the guidance and control software, an Attitude and Heading Reference System (AHRS), a Global Positioning System (GPS) receiver, and a heading-hold gyro. The standard off-the-shelf transmitter (the Futaba 9C Super), included with the basic system, is used as the ground controller for manual mode operation. A laptop, which runs the Ground Control System (GCS) software, is coupled with a joystick and a 900 MHz spread-spectrum (frequency hopping) modem shown in Figure 5-3, and provides semi-autonomous and full-autonomous flight capabilities. The camera gimbal is the E4 model from Helicam Solutions with retractable landing gear and gyro stabilized pan and tilt capability. The camera gimbal is controlled by an RC controller which is a Futaba 6EX operating at 2.4 GHz. The video camcorder is a Sony HDR-CX7 providing 1080p high definition video with internal flash memory storage and composite video output. The camcorder is connected to a RangeVideo 900 MHz FM video transmitter for downlink to the ground control station. At the ground control station, the video is encoded and connected to the wireless network allowing video access to security personnel.

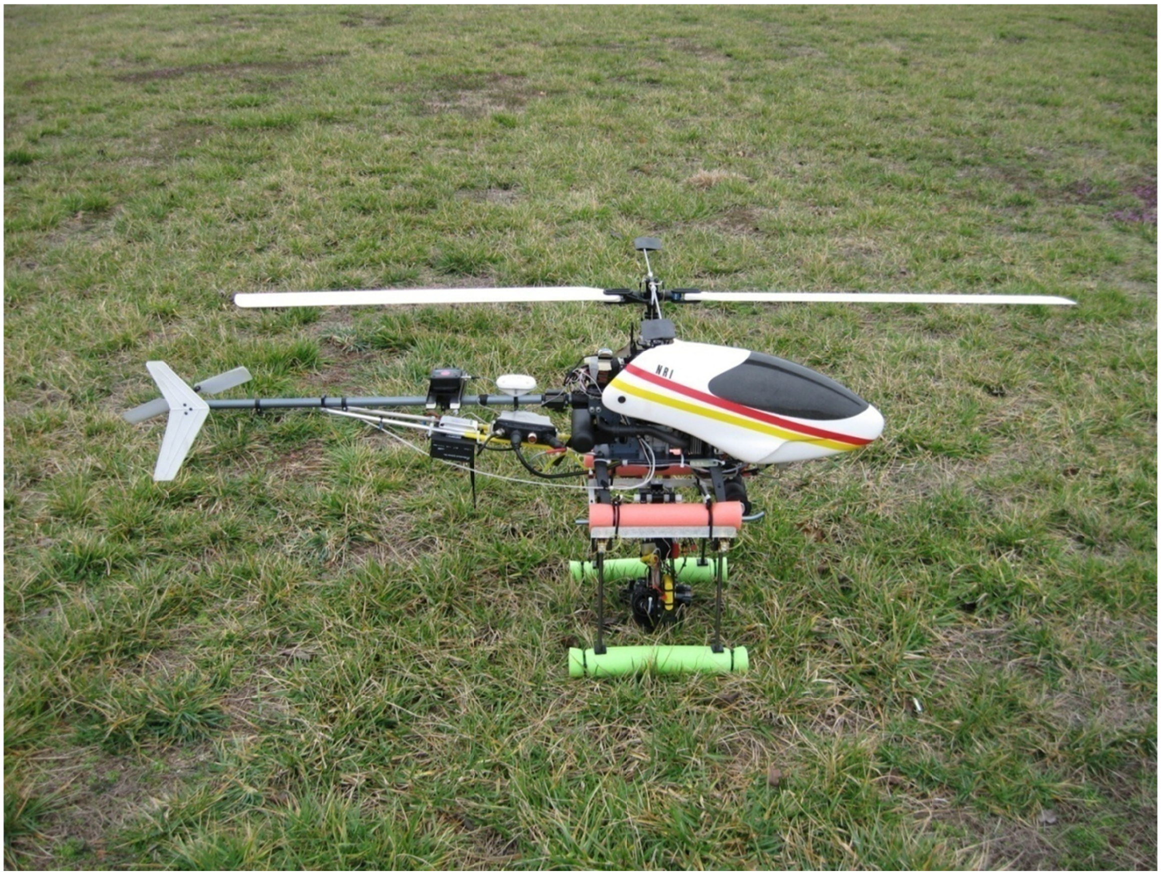


Figure 5-2. The Aerial Surveillance Vehicle used for the demo project.

A Vario Benzine trainer equipped with Global Positioning System, Altitude and Heading Reference System, Global Positioning System, modem, and Camera Gimbal.

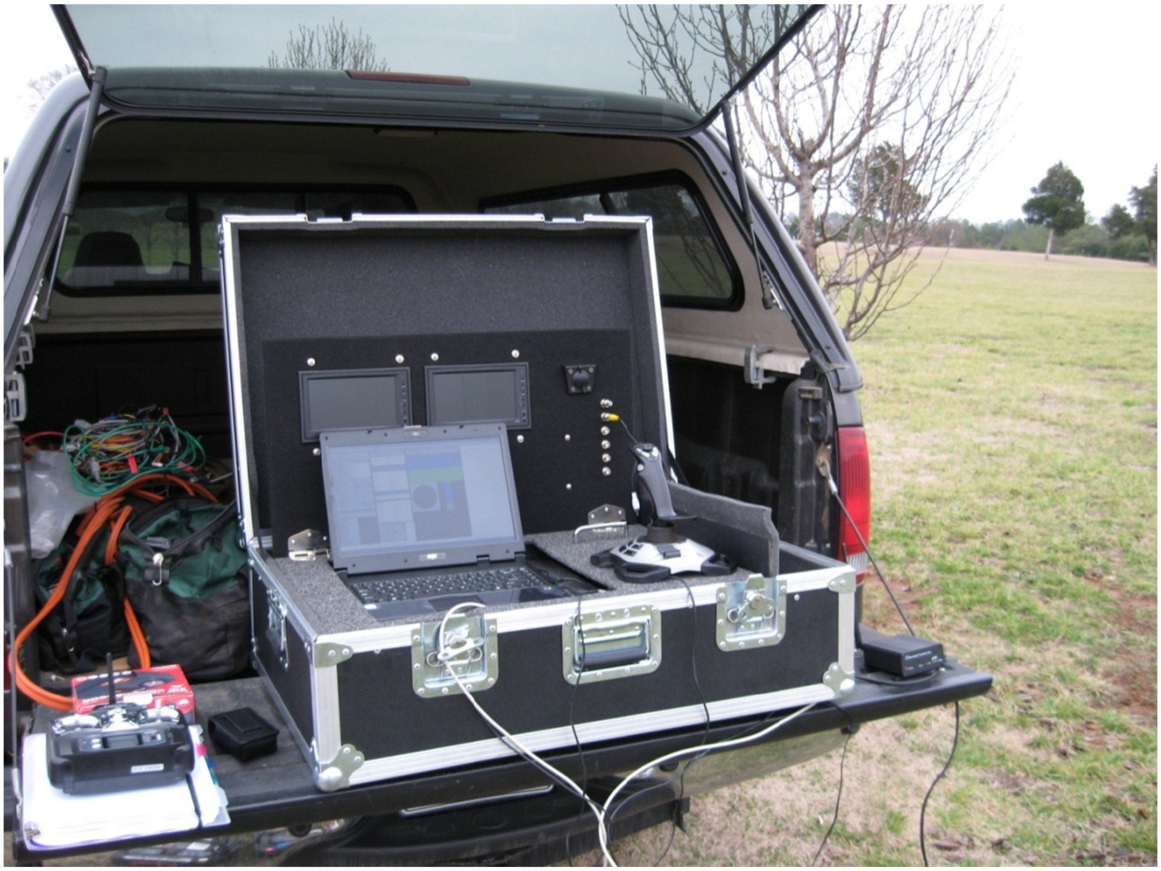


Figure 5-3. The ground control station for semi-autonomous and full-autonomous flight control of the aerial surveillance vehicle.

The laptop communicates joystick inputs to the ASV through a modem. Live video from the ASV is transmitted to the ground control station monitor for viewing.

Manual control of the aerial surveillance vehicle

In the manual flight control mode, the helicopter is simply a remote controlled vehicle. Pilot proficiency and situational awareness play a key role in the safe takeoff, flight, and recovery of the vehicle. Using the supplied RC controller, throttle, pitch, roll, and yaw can be controlled by the two joysticks to maneuver the helicopter to takeoff, fly to the designated area, hover, return, and land. In this mode, the helicopter requires constant operator input to maintain stable hover, thus requiring a second operator to control the video gimbal and camera. An additional RC controller is used to manually steer the gimbal mounted camcorder to provide the desired view with pan and tilt commands.

Autonomous control of the aerial surveillance vehicle

There are two modes of autonomous flight control, semi-autonomous and full-autonomous. Full-autonomous flight is accomplished without operator intervention after takeoff, while semi-autonomous requires basic operator input (or “direction”) throughout flight.

In the semi-autonomous mode, the ASV is self-stabilized using neural network-based flight control algorithms and inputs from the on-board avionics. In this mode, the GCS joystick provides basic high level flight control commands to the ASV such as; up, down, rotate left, rotate right, forward, and backward. The attitude and stability of the ASV is controlled by the onboard avionics and sensor suite. This is the mode that is demonstrated since it provides the most flexibility and ease of use in situations where situational dynamics are unknown (e.g., flight paths, areas of interest, and targets are dynamic based on the situation).

For the fully-autonomous flight mode, the ASV utilizes a GPS waypoint flight plan, where the operator uploads a flight plan to the ASV via a laptop computer, using GPS waypoints. In this mode, the operator starts the ASV, engages the Flight Control System (FCS), commands the ASV to take off and turns all flight operations over to the FCS. The operator can regain manual control of the ASV at any time by going back to the semi-autonomous mode. If the ASV flies out of RC range, the onboard avionics will turn the helicopter around and come back within range automatically.

5.2 - Results

The integration of the camera gimbal and helicopter provided a stable platform for demonstration of aerial video surveillance. Frequency conflicts between the ground control station and the video down link were quickly resolved with smart channel selection. RC controller conflicts with the NovAtel GPS receiver were catastrophic until it was realized that the GPS receiver sensitivity was such that during alignment, the RC controller, operating at 72 MHz prevented the GPS receiver from finding satellites. By having the operator maintain an acceptable distance from the ASV during the alignment process, this problem was quickly resolved.

In manual flight mode, the ASV performed as expected, constant operator input was required to maintain stable flight and hover. The gyro stabilized camera gimbal compensated for most ASV flight instability and produced acceptable video quality. Camera control was accomplished by a second operator. Figures 5-4, 5-5, and 5-6 show still images from the camcorder during manual flight. Image quality and resolution were adequate for security personnel to identify objects and individuals in the down linked video on the monitor.

In the semi-autonomous flight mode, the ASV performed flawlessly and helicopter control from the GCS was straight-forward. After arriving at the point of interest, releasing the joystick provided a stable hover through the FCS. Camera control was easily accomplished by use of the second controller while viewing the video on the GCS monitor. This video was encoded and transmitted over the wireless network and displayed at the security control center. During semi-autonomous flight, the camcorder's optical zoom capability provided the ability to resolve license plate numbers, container numbers and the security personnel were able to identify personnel at the demonstration area. Optical zoom has a negative effect by reducing the field-of-view producing the "soda straw" effect. This effect described in Kumar [20] and others, requires constant attention as objects of interest quickly move into and out of the image. Figures 5-7, 5-8, and 5-9 show images captured from the camcorder during semi-autonomous flight of the ASV.

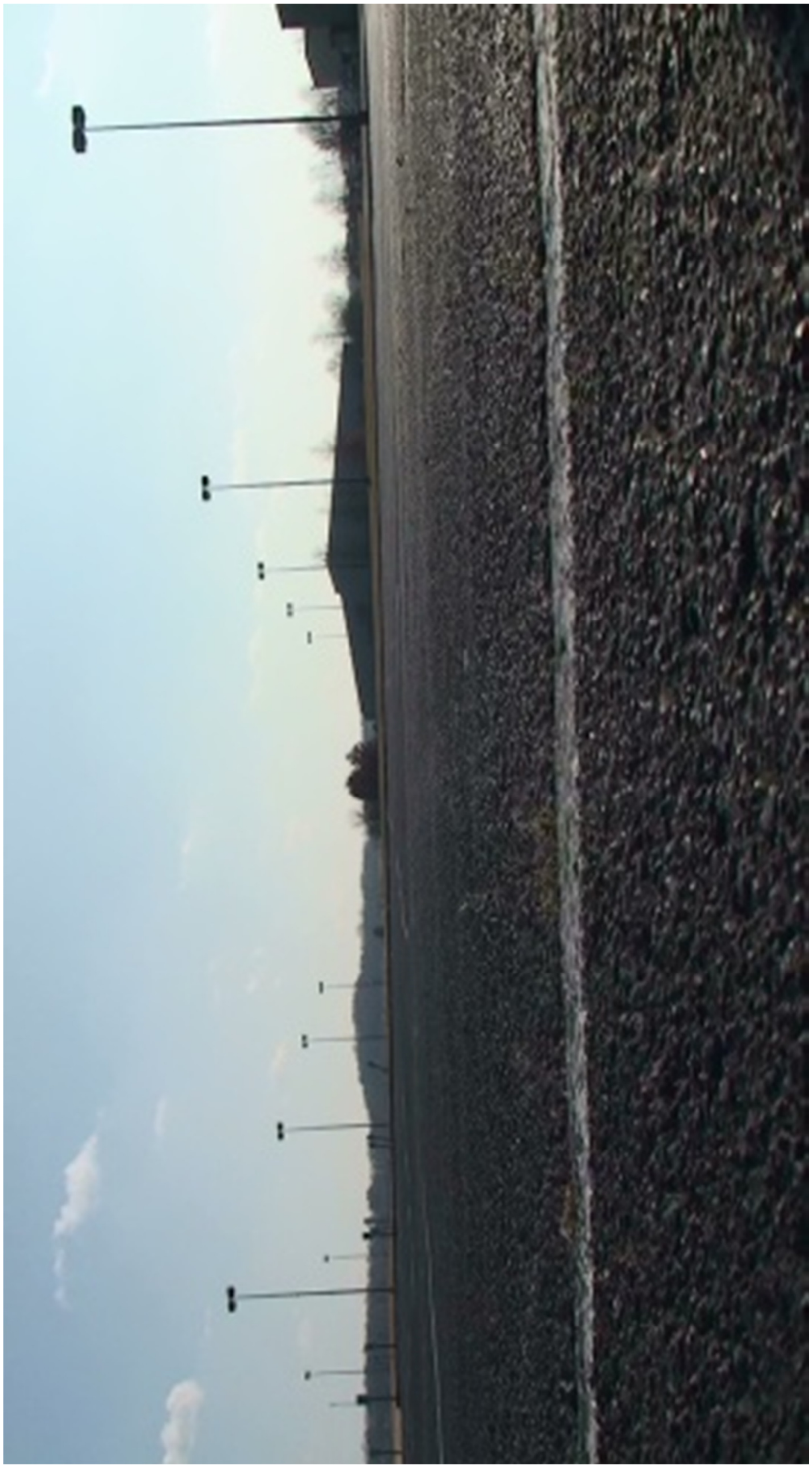


Figure 5-4. Image while the ASV is idling on the ground.

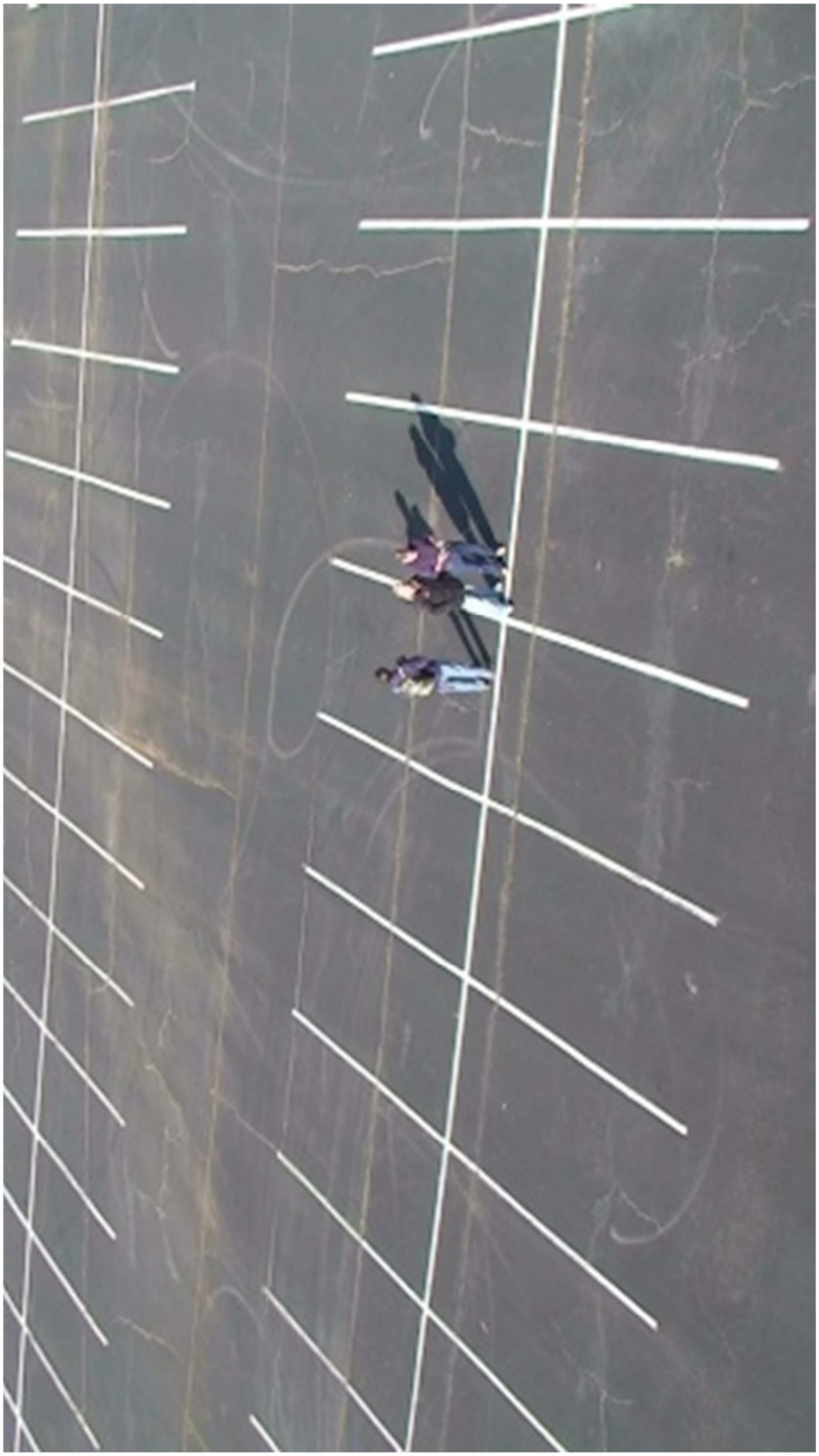


Figure 5-5. Image at 60 feet (18.3 meters) and 45 degrees of down camera angle.

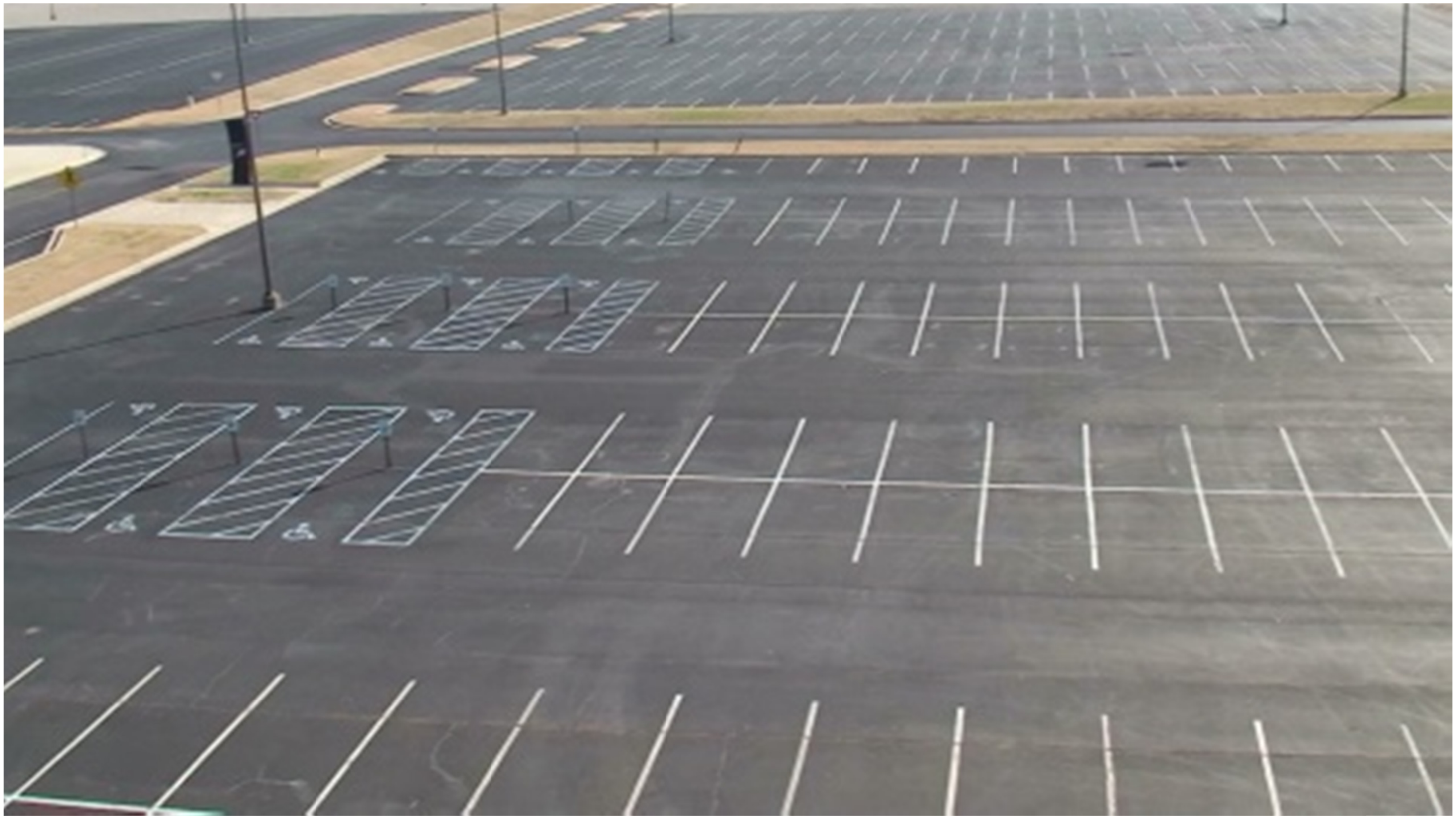


Figure 5-6. Image at 60 feet (18.3 meters) and 15 degrees of down camera angle.

Figure 5-7. Image while the ASV is idling on the ground.

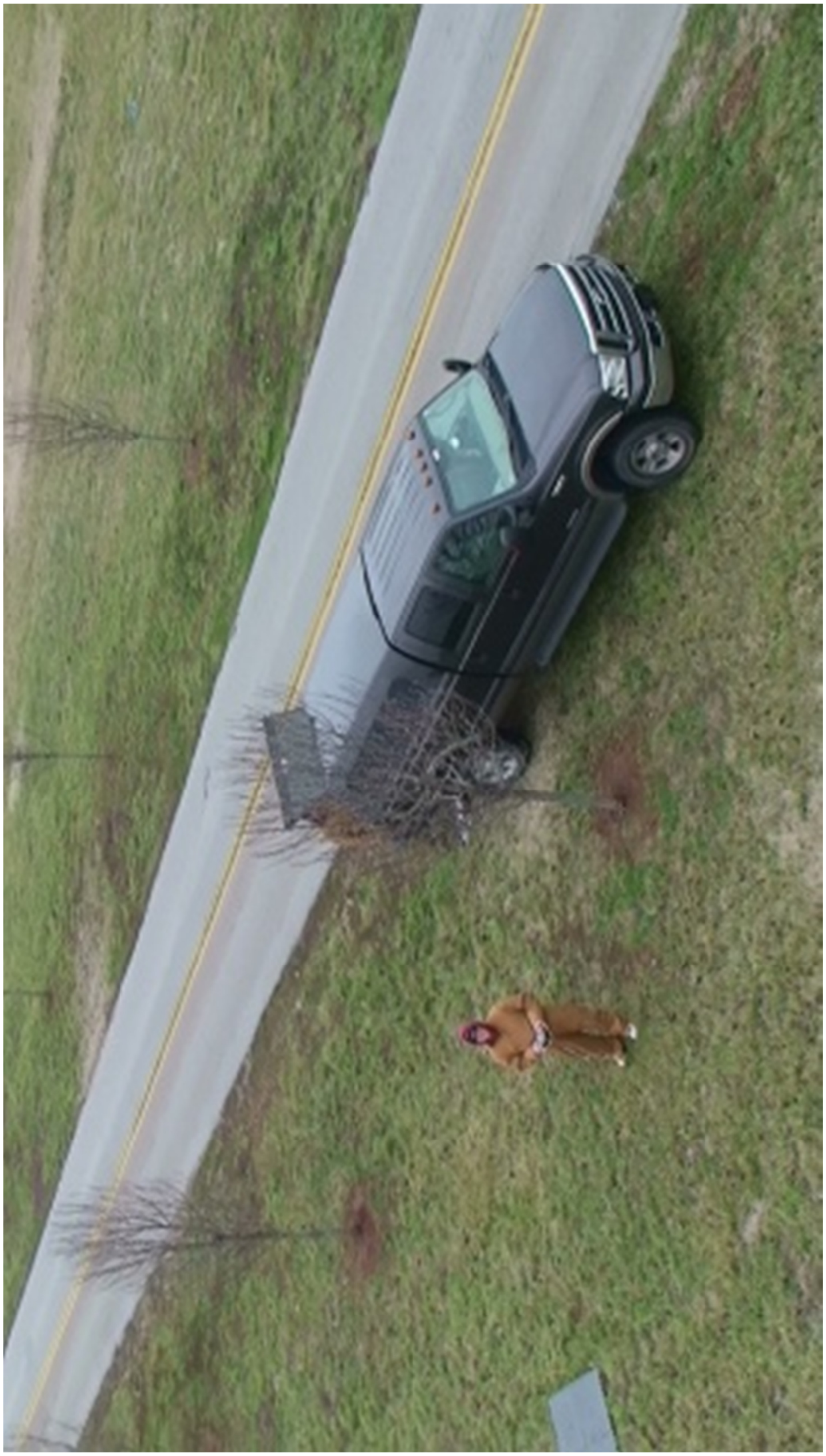


Figure 5-8. Image at 40 feet (12.2 meters) and 45 degrees of down camera angle.

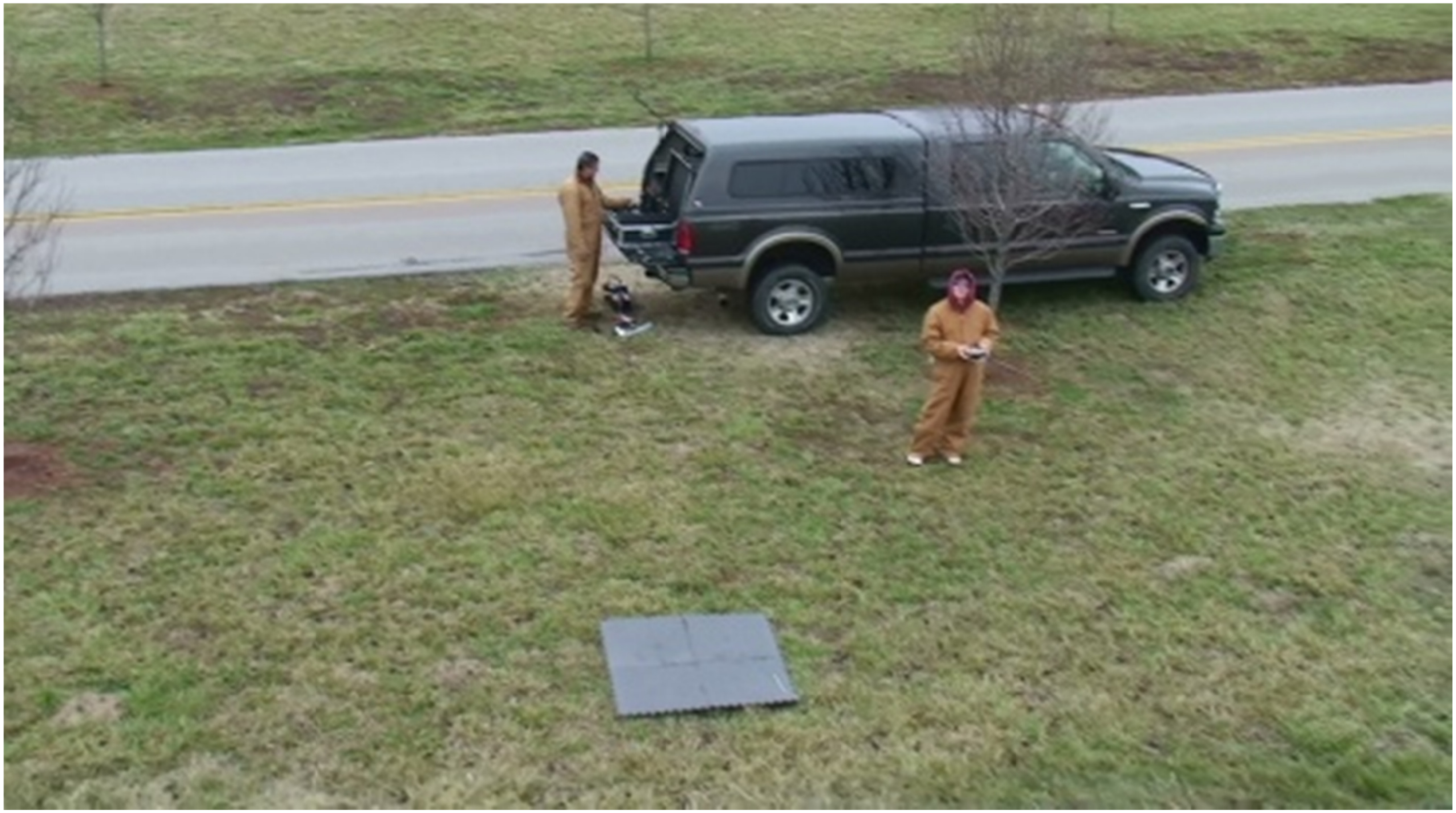


Figure 5-9. I**mage at 30 feet (9.1 meters) and 15 degrees of down camera angle.**

5.3 - Conclusion

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 research has demonstrated the use of aerial surveillance vehicles equipped with video cameras and wireless video downlinks to provide a birds-eye view of port facilities to security control centers and security patrols on the ground. This off-the-shelf capability can enhance existing security measures and help secure the port facilities. Future research is planned to link the full-autonomous flight capabilities of the ASV with GCS based object tracking and to provide interaction with other ground surveillance vehicles for autonomous surveillance.

Chapter 6 - ICFS Project Phase III Design

6.1 - 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 applications. These same benefits are applied 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 [21], [22].

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 [23]. 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 [24].

The author's previous research and deployment of a Statewide ITS Console [25] 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 system 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, communications 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, DMS*s*, Remote Traffic Detectors (RTDs), and RWS*s*.

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" [26]. 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 capable of both panning and zooming. It must support immediate jumping to predefined views. Where available, aerial photography will be overlaid 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 Oklahoma Department of Transportation (ODOT) Traffic Engineering and Maintenance Divisions, ODOT 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 RTD*s* is being deployed by Mobility Technologies, Inc. (www.traffic.com), and will provide traffic speed data for color coding roadway segments on the ITS Consoles and ATIS.

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 [27]. 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.) [28].

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.

6.2 - Development Project

This system 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.

6.2.1 - 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 eventually will 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 be deployed in a 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 communications 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 [29]. 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 STRIX™ system was chosen and has thus far proven reliable for the application. Access points will be installed on camera poles where fiber optic cables are available and subscriber modules will be installed at the remote devices. The STRIX™ system provides 54 Mbps of bandwidth point-to-point with a range of two miles (3.2 km).

A single STRIX™ link provides device control simultaneously with acceptable video quality for multiple CCTV camera video streams and multiple IP web camera video streams.

The architecture of the distributed IP network is shown in Figure 6-1. In addition to video streams, communication with devices including control and data acquisition for RTD*s* and RWS*s* 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.

6.2.2 - 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:

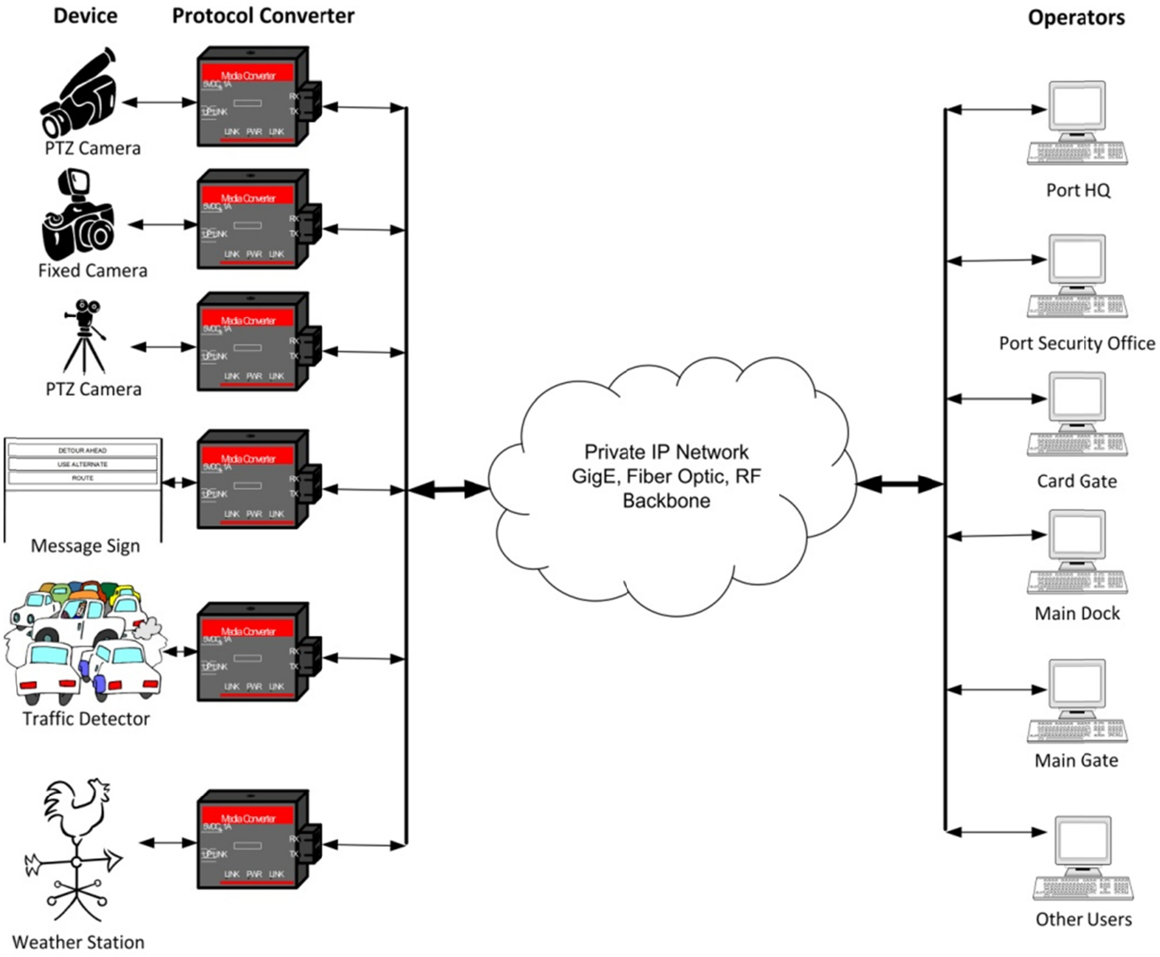


Figure 6-1. Distributed IP network architecture.

- 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 DMS*s*, and of controlling, configuring, and acquiring data from RTD*s*, RWS*s*, 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.

6.3 - Conclusion

This Chapter briefly described the main features of the statewide ITS that is currently deployed in Oklahoma 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.

Chapter 7 - ICFS Project Phase III Implementation

7.1 System Demonstration

Phase 3 of the Intermodal Containerized Freight Security project is to install a prototype system at the Port-of-Catoosa, and demonstrate the functionality of the system. During this phase, a prototype demonstration using COTS technology and custom software will be provided. The research leading to this demonstration also has resulted in field tested hardware and software configurations in a variety of settings and conditions.

7.1.1 Concept

Based on work from the development of a Statewide Intelligent Transportation System [5], a simplified approach to system integration is demonstrated. This ITS work has continued to be enhanced over the years with little change to the architecture foundation, demonstrating the robustness of the concept [30]. The author's research and deployment of a Statewide ITS Console [25] is distinct from previous distributed control architectures in that it provides the complete functionality of a centralized control center and does not require any specialized equipment. Any single instance of the ITS Console is capable of functioning independently as a control center 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.

7.1.2 Design

For the port project, 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 [31]. The software packages identified in Chapter 6 will be used to support the operator console main application software.

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 video, of controlling the PTZ cameras, and of controlling, configuring, and acquiring data from 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.

The software architecture, shown in Figure 7-1, is similar to the Intelligent Transportation System described in [5]. The database includes tables that contain all the necessary system information. Tables for the devices, device locations, device command sets and sensor data sets are created to include all data vital for the overall system. The database interfaces with the application software by an ODBC table adapter. This table

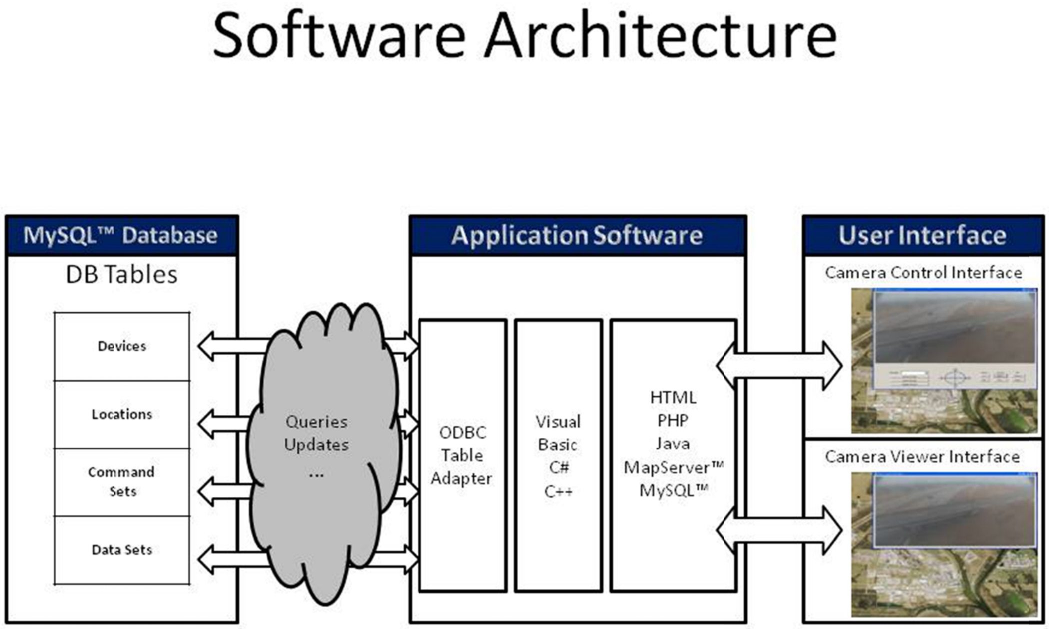


Figure 7-1. **Overall software architecture**

adapter carries all the queries and updates back and forth from the database to the application.

Software

On the application side, several programming languages are used to interoperate with the system database and the user interface. For example, VB.NET is used to create the "Camera Viewer" which is a graphical user interface that gives the console operator access to the live video feed of a camera situated at the port. Another example would be using the PHP script. The dynamic web interface that shows the map of the Port of Catoosa is created using PHP script. On this interface, the user will be able to choose to view different live video feeds at different locations. The use of various programming languages gives more freedom for the developers to choose the best language to fit the task in hand.

The last part of the software architecture is the user interface. This interface allows the user to view and control different devices. There are two types of users: limited access user and advanced user. Limited access users are only allowed to view the data request results. On the other hand, advanced users can view, update, and modify all of the system's data sets.

The overall architecture of the software hosts various applications that can run on any console. The only requirement for the console to execute the application commands is to be connected to the system. The surveillance system is interconnected and can be accessed by authorized personnel from any console. This network connection provides users the capability to monitor and configure all of the sensors and devices present at the port.

As shown in Figure 7-2, the application handles two types of inputs: a triggered event and a user request. A triggered event is executed whenever an alert goes off. Alerts can be the result of sensors readings, motion detection, etc. A user request is generated through the user interface.

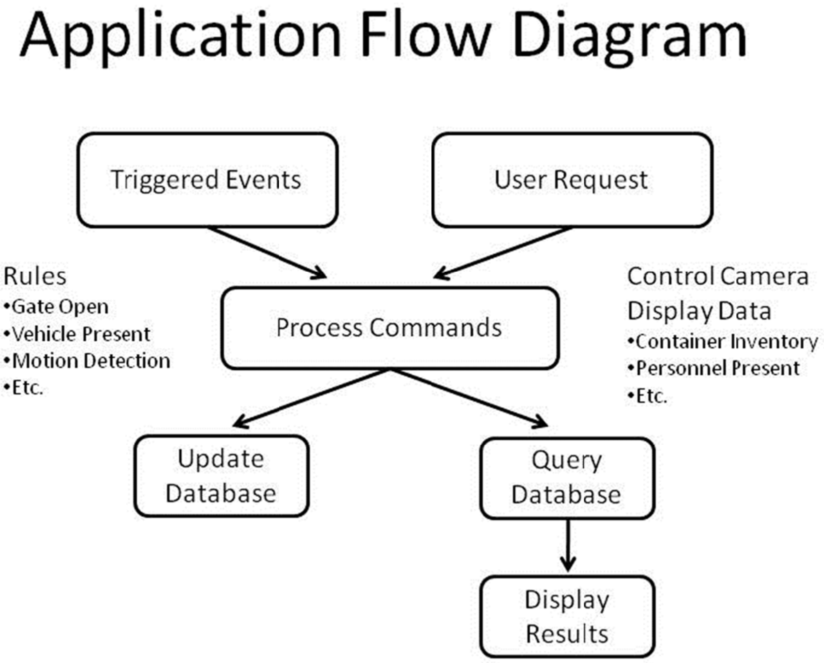


Figure 7-2. A flow diagram of the system application

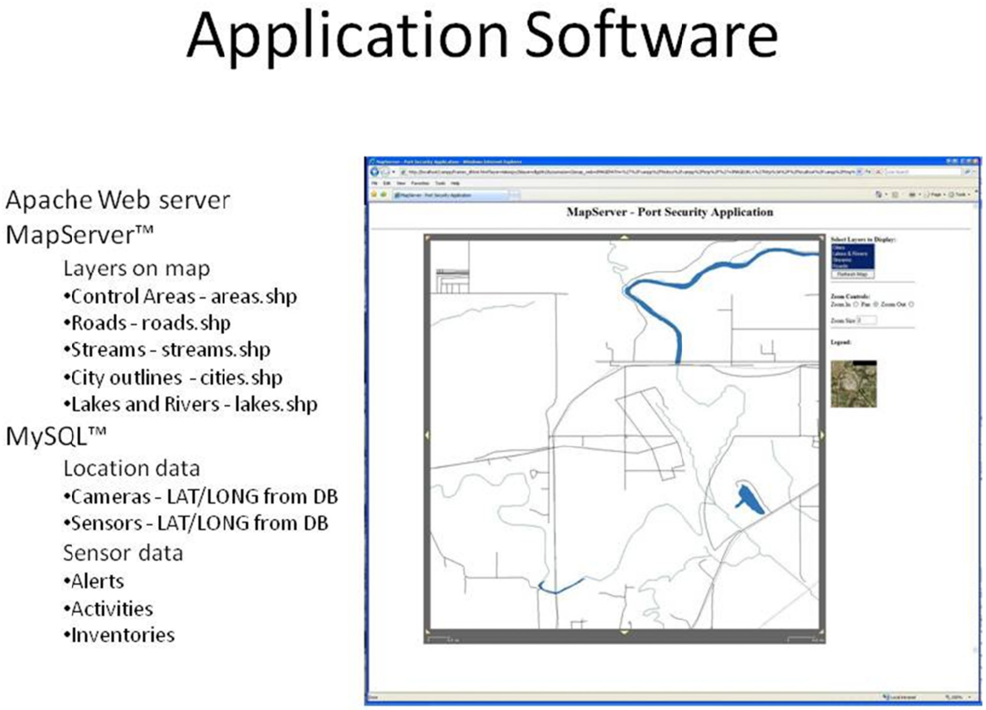
Commands based on user input or triggered events are handled by the processor. The latter makes decisions to control, update, or query data sets. For example, if a command is sent by the user to tilt camera 2, then the application receives that command and queries the database to get the specific command for that camera. The application then sends the command to camera.

Some of the messages received by the console are update messages. In that case, the console only updates the database with no further action taken. If the request includes displaying results, such as a live video feed, the console first finds which device to interrogate by querying the database. Then, the console sends a command to it to retrieve the required information from the device and finally display it to the user.

The application is made to serve different makes and models of different sensors and devices. Thus, adding new equipment to the overall system should not be a troublesome approach. The application will require few updates to the database and some minor additions to the main code.

The application software contains an interactive web interface supported by an Apache web server. The application provides the user with a map of the port with several optional features. The user can find on the map the different locations where cameras are located and view live video captures. If the user is given adequate privileges, he/she can view and control the cameras. Upon selection, the user can control a PTZ camera, for example, and be able to set different parameters for a better use of the camera. The application software will also alert the user of any problems monitored by the overall system.

The map shown in Figure 7-3 is a sample of the Port Software Application. The user is able to move the cameras to any desired location. The user can also select different layers to add to the map, those include: control areas, roads, streams, city outlines and lakes and rivers. Adding these layers facilitates viewing several regions of the port. A legend of the map is present to quickly redirect the user to the port location in case they shift to another area in the map.



Application Software

- Apache Web server
- MapServer™
  - Layers on map
    - •Control Areas - areas.shp
    - •Roads - roads.shp
    - •Streams - streams.shp
    - •City outlines - cities.shp
    - •Lakes and Rivers - lakes.shp
- MySQL™
  - Location data
    - •Cameras - LAT/LONG from DB
    - •Sensors - LAT/LONG from DB
  - Sensor data
    - •Alerts
    - •Activities
    - •Inventories

MapServer - Port Security Application
Select Layers to Display:
Cities
Lakes & Rivers
Streams
Roads
Refresh Map
Zoom Controls:
Zoom In ○ Pan ◉ Zoom Out ○
Zoom Size 3
Legend:

Figure 7-3. A view of the Port Software Application

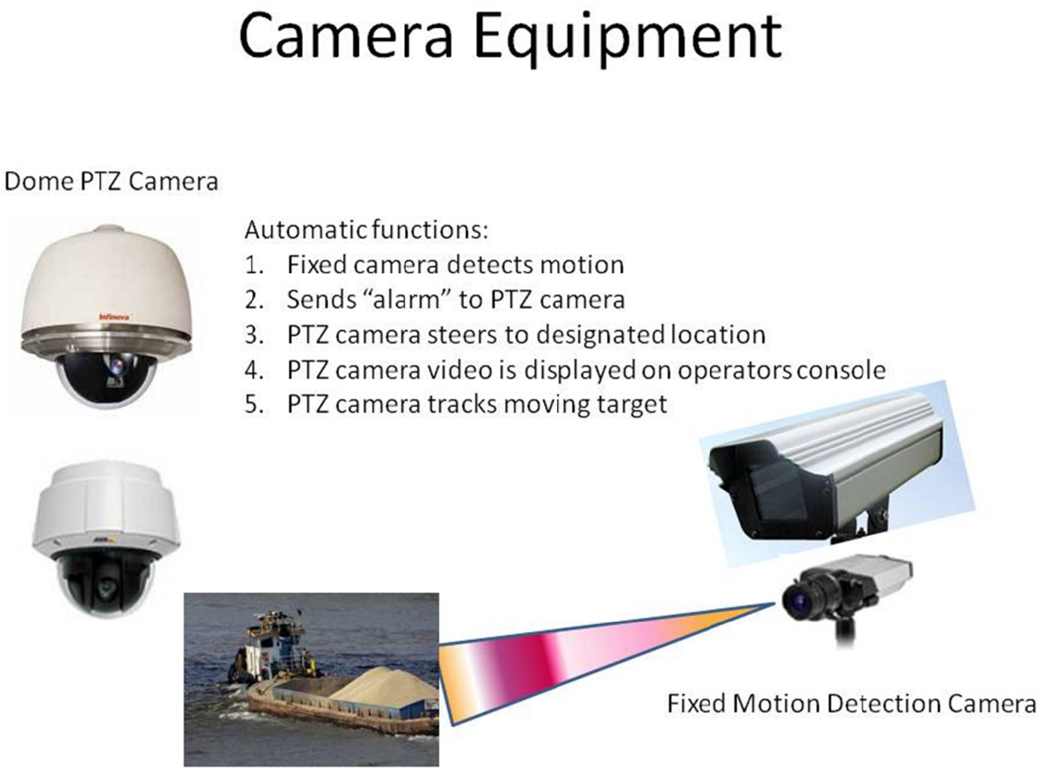
All the information present on the map is stored in the database, as well as all the changes that are sent as updates to the data tables. The database also contains: locations of the cameras and sensors, and sensor data, such as alerts, activities and inventories. When an alert goes off, the user is alarmed and the database is updated accordingly. User inputs generate commands that are sent through the network, these commands are also stored in the database.

The overall system is built to convey interoperability among different kinds of equipment. One example of interoperability is the use of different makes and types of cameras. The system is capable of easily adding new models of cameras and integrating them to function as desired.

At the port, two types of cameras are used: fixed cameras and PTZ (Pan, Tilt, and Zoom) cameras (Figure 7-4). The fixed cameras are split into two categories: the ones with motion detection and the ones without. Motion detection is considered as a triggered event that interrupts ongoing system processes. Alarms coming from static cameras are also used to move PTZ cameras to the desired site so that the user can then direct the PTZ accordingly.

The PTZ cameras are also capable of performing motion detection and tracking in either of the cases: an event triggered by a fixed camera or motion detection in the surveillance area. The operator's console shows all feeds from the fixed and PTZ cameras. The operator can then subjectively analyze the live video. The system automatically triggers alarms upon motion detection and thus can alert the operator of any suspicious acts.

The idea of motion detection and tracking can be expanded into recognizing the moving objects. A study is in process to perform accurate human detection and tracking at the port. This study, A Personnel Detection Algorithm for an Intermodal Maritime Application of ITS Technology for Security at Port Facilities [32], will enable detection of unauthorized personnel in secure area. It will also give the system a more intelligent



Camera Equipment

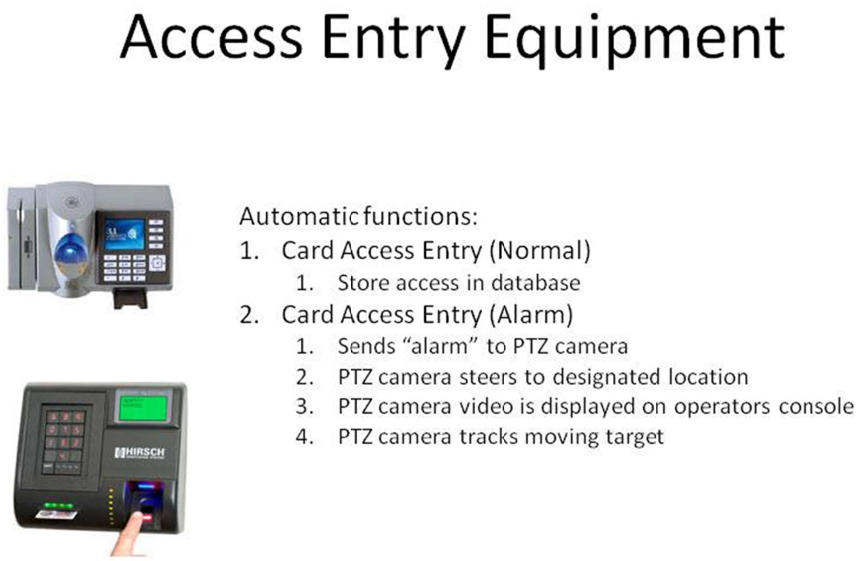
Automatic functions:

1. Fixed camera detects motion
2. Sends "alarm" to PTZ camera
3. PTZ camera steers to designated location
4. PTZ camera video is displayed on operators console
5. PTZ camera tracks moving target

Figure 7-4. Types of cameras used at the port

aspect in finding unwanted people. Human detection and tracking is a well known computer vision challenge that different researchers have put plenty of work into [33].

Access entry equipment is present in areas where security levels are very high. Such areas, for example cargo storage areas, are under surveillance 24/7 (Figure 7-5). Only authorized people are given access in and out from these areas. There are different types of devices that can be used to authorize certain individuals. Some examples of that



Access Entry Equipment

Automatic functions:

1. Card Access Entry (Normal)
    1. Store access in database
2. Card Access Entry (Alarm)
    1. Sends “alarm” to PTZ camera
    2. PTZ camera steers to designated location
    3. PTZ camera video is displayed on operators console
    4. PTZ camera tracks moving target

Figure 7-5. Type of access entry equipment used at the port

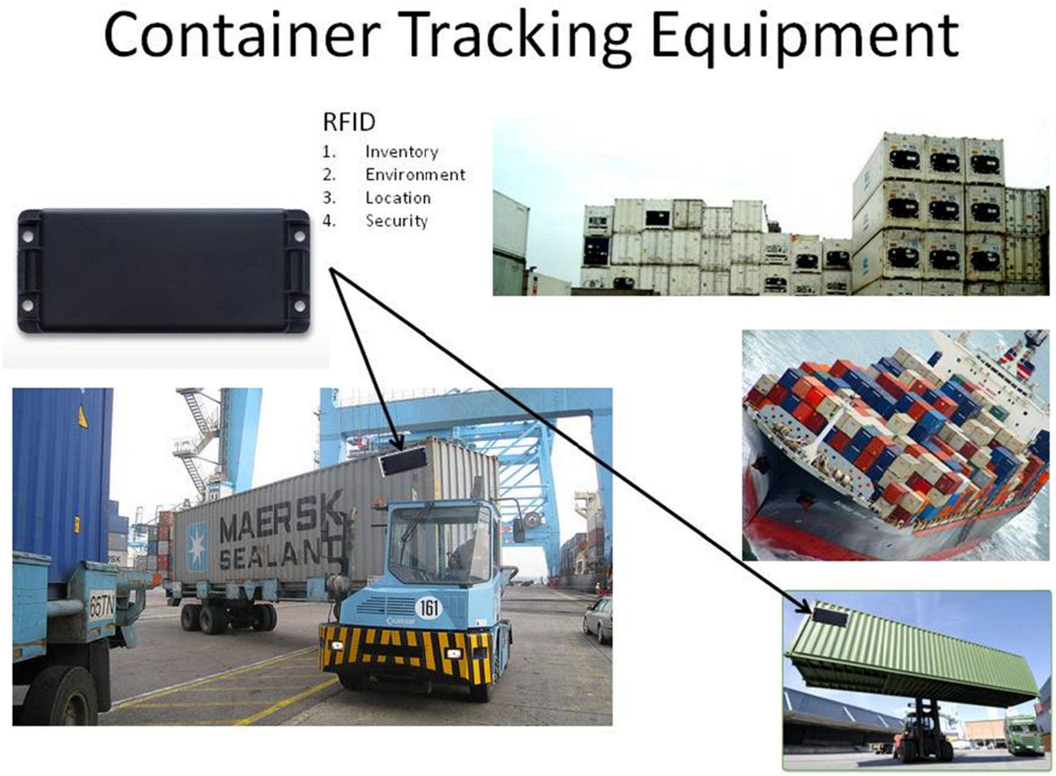
are: finger print access entry devices and card access entry devices. The equipment used at the port are card access entry devices that read tags of the access cards.

Whenever an individual uses an access card, an assigned PTZ camera will move automatically to give a live preview of the current user. This helps authenticate users in a more efficient and safe way. An event of a card read by the access entry device triggers a designated PTZ camera to show the operator the detailed scene of what is happening. This easy to manage approach replaces the need to have operators perform a long subjective analysis of current video feedbacks from a variety of cameras. After moving the PTZ camera to the desired scene, the camera again takes over and starts tracking the moving targets. Unless interrupted by another user command or a higher priority alarm, the PTZ camera will keep on tracking the detected target.

Some types of the access card readers can read up to 6 inches away from its sensing area. Usually, the tag found on the access card is a passive circuit and does not contain any active chips. Unless the user gets close enough to be authenticated by the reader, no access is given.

While millions of containers are shipped to the United States on a yearly basis, not much information is given about each container. Attaching RFID devices, as shown in Figure 7-6, can collect sensory data about the conditions of the container can be very beneficial. Sensors are used to measure humidity, temperature, light intensity, door locked/unlocked, etc. Thresholds of these measurements are used to sound off alerts to the console. For example, a container can be carrying some type of food that requires certain degrees of temperature to be preserved. If the temperature, at any time, exceeds that limit an alert will be sent out to the RFID device.

This facilitates the process of keeping a suitable environment inside the container for goods safety. Door lock sensors are very important to report any alteration of the container from its source to destination. The sensors help maintain a protective environment of what is inside the container.



Container Tracking Equipment

RFID

1. Inventory
2. Environment
3. Location
4. Security

Figure 7-6. Proposed wireless container tracking equipment.

(Image source - MAERSK Line web site)

Monitoring each container strengthens the container security and provides valuable information. All this data in addition to location data can then be stored in the database. As ships or barges enter the port network, the RFID devices start data transfers to the system. Information about all the containers are collected and analyzed by the console operator. The location data informs the operator of the current position of the container after it is put in a staging area at the port. Any relocation of the container can be monitored from the console. This helps locate containers if present in the staging area before being shipped out from the port itself.

The process of reading all the RFID devices off the containers can be a long process if a huge load is being carried by the ship or barge. Reading the RFID devices starts at the moment the ship/barge enters the port coverage area. From that point and until all the containers are stored, the RFID reader will have enough time to complete the process.

Hardware

The architecture of the distributed IP network is shown in Figure 7-7. In addition to video streams, communication with devices including control and data acquisition for sensors 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.

Existing technology makes it extremely easy to create a fault tolerant network that can handle multiple streams of video, data, and sensor commands. Reaching locations that do not have existing infrastructure can have wireless access installed with high-bandwidth and encryption to accommodate the location and equipment. Careful planning can ensure redundancy in the network and therefore console access and equipment control in achieved.

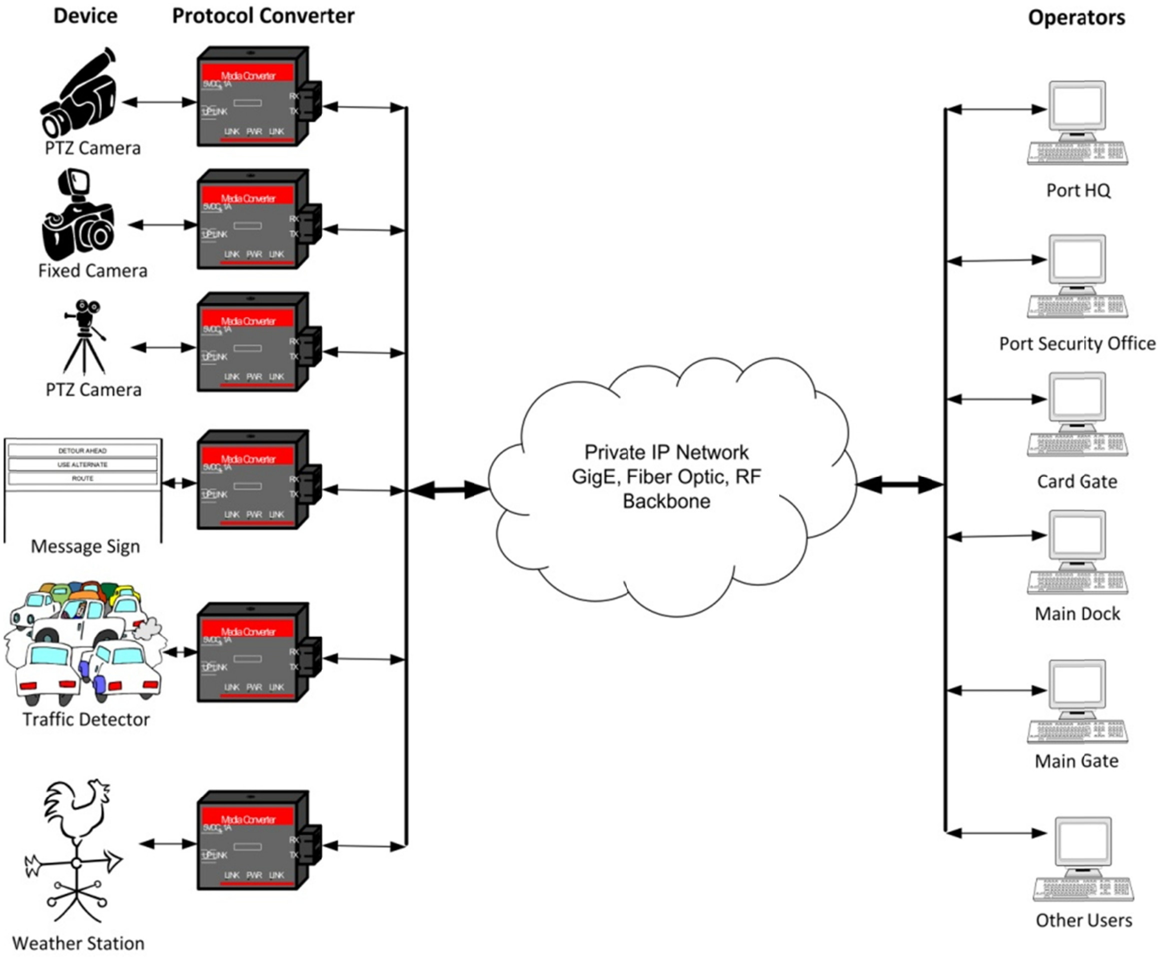


Figure 7-7. Distributed IP network architecture.

7.2 Conclusion

Port security is essential for maintaining safe and efficient movement of cargo. In these times of slim budgets, new and innovative approaches must be considered and implemented. The Inter-modal Containerized Freight Security project has demonstrated many existing technologies and found a few holes that can be fixed. Port security is achievable and can be cost effective. Through this use of off-the-shelf hardware and software, an efficient and low cost security system was developed and installed at the Port of Catoosa.

This building block approach to security systems will enable the system to grow with the port without having to rebuild it from the ground up, thus saving time and money. Additionally, as new technologies come to market, the software architecture allows additional device handlers to be added without changing the core software. This design reduces maintenance costs and burdensome retesting and requalification of existing software.

Chapter 8 - Software Design

For any system to function, software plays a critical role and good design practices and planning are very important. This demonstration project is no different; software development needs to follow a structured path to reduce future maintenance costs associated with adding additional functionality. The software architecture used for this project has benefited by incorporating lessons learned from previous projects.

Some of these lessons include:

- Create modules that can extract data from a database to manipulate their behavior.

  This reduces software development and maintenance costs.

- Create modules that perform a single function.

  This simplifies software development.

- Create modules that do not require retest when other parts of the system are changed.

  This reduces software maintenance costs.

Since all devices in the system are connected to the network, either directly, through a terminal server, or through a protocol converter, all devices in the system will have two attributes that are the same regardless of their function. These attributes are an IP address for controlling them, and an IP addresses for collecting data from them. The data collected can be a video stream or a data stream.

The following code example was developed to extract the control IP address from the database for the device that is requested to be controlled. In this case, the device is a camera, but this code will work to extract the control IP address for any device type that exists in the system.

```
Private Sub getControlIPFromDb()
        'Open a connection to the database
        mysqlconn.Open()
        command.Connection = mysqlconn
        'Query the database for the control IP address
        command.CommandText = "select camControlIP from camera where camID = "
                & camID & ";"
        'Read the results
        Dim mysqlreader As MySql.Data.MySqlClient.MySqlDataReader =
                command.ExecuteReader(CommandBehavior.SingleResult)
        mysqlreader.Read()
        'Assign the control IP address to the used variable
        controlIP = mysqlreader.Item(0)
        'Close the database reader and then connection
        mysqlreader.Close()
        mysqlconn.Close()
        End Sub
```

The following code example was developed to extract the video IP addresses from the database for the camera that is requested to be viewed. But again, it will work to extract the control IP address for any device type that exists in the system.

```
Private Sub getVideoIPFromDb()

        'Open a connection to the database

        mysqlconn.Open()

        command.Connection = mysqlconn

        'Query the database for the video IP address

        command.CommandText = "select camVideoIP from camera where camID = "

                & camID & ";"

        'Read the results

        Dim mysqlreader As MySql.Data.MySqlClient.MySqlDataReader =

                command.ExecuteReader(CommandBehavior.SingleResult)

        mysqlreader.Read()

        'Assign the video IP address to the used variable

        videoIP = mysqlreader.Item(0)

        'Close the database reader and then connection

        mysqlreader.Close()

        mysqlconn.Close()

        End Sub
```

ActiveX controls are like mini program building blocks and can serve to create distributed applications working over the network. Some examples of these ActiveX controls include customized applications for collecting data, viewing data in a useable format, and displaying video. Many device manufacturers provide these ActiveX controls with their hardware to reduce the hardware integration effort. If the device is a legacy piece of equipment, this ActiveX control will need to be developed, or at the very least, an interface software module to collect the data and convert it into a useable format will be required.

The following code example is one of the critical functions to reducing the software maintenance of this system. Based on the type of device that is selected for control, the database is queried to determine the name of the ActiveX control that is required to operate the requested piece of equipment. By getting the ActiveX control name from the database, the ActiveX control can be spawned and critical information can be passed to it without ever knowing which control is being used. This example is for a camera that is requested to be viewed. But again, it will work to extract the ActiveX control for any device type that exists in the system.

```
Private Sub getActiveXFromDb()

        'Declare the array of strings

        Dim parsingstr As String() = Nothing

        'Open a connection to the database

        mysqlconn.Open()

        command.Connection = mysqlconn

        'Query the database for the ActiveX type and method

        command.CommandText = "select activexType, activexMethod

                from camera where camID = " & camID & ";"

        'Read the results

        Dim mysqlreader As MySql.Data.MySqlClient.MySqlDataReader =

                command.ExecuteReader(CommandBehavior.SingleRow)

        mysqlreader.Read()

        'Assign the ActiveX type and method to the used variables

        ActiveXType = mysqlreader.Item(0)

        ActiveXMethod = mysqlreader.Item(1)

        'Close the database reader and then connection

        mysqlreader.Close()

        mysqlconn.Close()

        End Sub
```

The following code example was developed to extract the make from the database for the camera that is requested to be viewed. But again, it will work to extract the make for any device type that exists in the system.

Knowing the make of a device can enhance the user experience by providing some details about the device it the control Graphical User Interface (GUI).

```
Private Sub getMakeFromDb()

    'Open a connection to the database

    mysqlconn.Open()

    command.Connection = mysqlconn

    'Query the database for the camera make

    command.CommandText = "select camMake from camera where camID =

        " & camID & ";"

    'Read the results

    Dim mysqlreader As MySql.Data.MySqlClient.MySqlDataReader =

        command.ExecuteReader(CommandBehavior.SingleRow)

    mysqlreader.Read()

    'Assign the camera make to the used variable

    cMake = mysqlreader.Item(0)

    'Close the database reader and then connection

    mysqlreader.Close()

    mysqlconn.Close()

    End Sub
```

The following code example was developed to extract camera presets from the database for the camera that is requested to be viewed.

```
Private Sub getPresets()

        'Define the counter for the loop

        Dim i As Integer = 0

        'Enter a loop to retrieve all the stored presets

        For i = 0 To 127

        'Open a connection to the database

        mysqlconn.Open()

        command.Connection = mysqlconn

        'Query the database for the camera make

        command.CommandText = "select preset" & i & " from cam_presets

                where camID = " & camID & ";"

        'Read the results

        Dim mysqlreader As MySql.Data.MySqlClient.MySqlDataReader =

                command.ExecuteReader(CommandBehavior.SingleRow)

        mysqlreader.Read()

        'Check if the reader returned a Null

        If mysqlreader.IsDBNull(0) OrElse mysqlreader.Item(0) = "NULL"

        Then

                savedPresetsArray(i) = "NULL"

        Else

                'Assign the camera presets to the used variable

                savedPresets = mysqlreader.Item(0)
                presets.Items.Add(savedPresets)

                savedPresetsArray(i) = savedPresets

        End If

        mysqlreader.Close()

        mysqlconn.Close()

        Next

        End Sub
```

The following code examples are representative of single function software design that can query the database for all necessary data without having to know about the actual hardware being controlled. To control a device, the system must be able to detect the press down of the mouse button and the release of the mouse button to know the duration of the command to be issued to the device.

```
Private Sub PanRight_MouseDown(ByVal sender As Object, ByVal e
        As System.Windows.Forms.MouseEventArgs) Handles PanRight.MouseDown
        cmd = "panRight"
        t = Type.GetType("PortCameraControl." & cMake & "CmdBuilder")
        t.InvokeMember("cmdBuild", BindingFlags.InvokeMethod Or
                BindingFlags.Public Or BindingFlags.Static, Nothing, Nothing,
                New Object() {camID, controlIP, cmd})
        End Sub

Private Sub PanRight_MouseUp(ByVal sender As Object, ByVal e
        As System.Windows.Forms.MouseEventArgs) Handles PanRight.MouseUp
        cmd = "panStop"
        t = Type.GetType("PortCameraControl." & cMake & "CmdBuilder")
        t.InvokeMember("cmdBuild", BindingFlags.InvokeMethod Or
                BindingFlags.Public Or BindingFlags.Static, Nothing, Nothing,
                New Object() {camID, controlIP, cmd})
        End Sub
```

As mentioned previously, the databases are critical to the system should contain enough information to be able to provide the software with all parameters necessary to collect data or control a device. This includes commands that can be concatenated with control strings in the ActiveX control to create commands that the device understands. It can be location information, or logical addresses as well as model number, serial number, and other manufacturer information.

Figure 8-1 illustrates the design flow for adding a new device to the system. If a new sensor is added, it will require a new ActiveX control or equivalent interface module and sensor unique information for the database that provides addressing and control information.

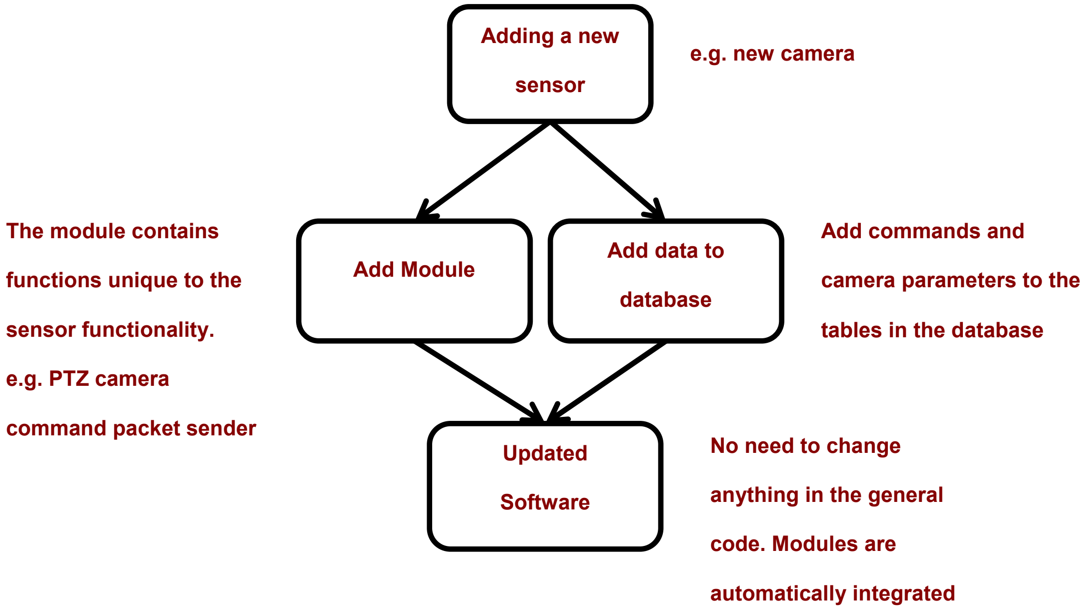

Adding a new sensor
e.g. new camera
The module contains functions unique to the sensor functionality. e.g. PTZ camera command packet sender
Add Module
Add data to database
Add commands and camera parameters to the tables in the database
Updated Software
No need to change anything in the general code. Modules are automatically integrated

Figure 8-1. Design flow for adding a new device to the system.

For the cameras in this system, there are four databases: camera, command_set, camlist, and location. The database schema for these tables is provided below.

`camera` database

```
`camID` varchar(10) NOT NULL COMMENT 'Camera ID'
`locID` varchar(10) NOT NULL COMMENT 'Location ID'
`recordTime` datetime DEFAULT NULL COMMENT 'Date and Time of the record'
`camLogicalID` varchar(15) NOT NULL DEFAULT '1'
`camVideoIP` varchar(15) DEFAULT NULL COMMENT 'The IP address of the camera video'
`camControlIP` varchar(15) DEFAULT NULL COMMENT 'The IP address of the camera control'
`camType` varchar(10) DEFAULT NULL COMMENT 'Camera Type'
`camMake` varchar(25) DEFAULT NULL COMMENT 'Camera Make'
`camModel` varchar(25) DEFAULT NULL COMMENT 'Camera Model'
`activexType` varchar(30) DEFAULT NULL COMMENT 'Activex needed for camera'
`activexMethod` varchar(30) DEFAULT NULL
`camSource` varchar(50) DEFAULT NULL COMMENT 'The source link for the camera'
`vidHeight` int(11) DEFAULT NULL COMMENT 'The height of the video'
`vidWidth` int(11) DEFAULT NULL COMMENT 'The width of the video'
`priority` tinyint(1) DEFAULT NULL COMMENT 'High priority (True/False)'
`trigger` tinyint(1) DEFAULT NULL COMMENT 'Is this camera triggering another camera'
`slave` varchar(50) DEFAULT NULL COMMENT 'Who is controlling this camera'
`isControlled` tinyint(1) DEFAULT NULL COMMENT 'Is camera controlled'
`userID` varchar(10) DEFAULT NULL COMMENT 'User Id of the camera in conrol'
`status` varchar(10) DEFAULT NULL COMMENT 'Camera status (running, idle, broken)'
`motionDetection` tinyint(1) DEFAULT NULL COMMENT 'Is motion detection enabled'
`autoTracking` tinyint(1) DEFAULT NULL COMMENT 'Is auto tracking enabled'
```

`camlist` database

`camId` varchar(5) NOT NULL

`locName` varchar(100) NOT NULL

`description` varchar(100) NOT NULL

`url` varchar(100) NOT NULL

`url2` varchar(100) NOT NULL

`latitude` float NOT NULL

`longitude` float NOT NULL

`command_set` database

`comSetID` varchar(10) NOT NULL COMMENT 'Command Set ID'

`camID` varchar(10) DEFAULT NULL COMMENT 'Camera ID'

`recordTime` datetime DEFAULT NULL COMMENT 'Date and Time of the record'

`camMake` varchar(25) DEFAULT NULL COMMENT 'Camera make'

`camModel` varchar(25) DEFAULT NULL COMMENT 'Camera Make'

`panRight` varchar(100) DEFAULT NULL COMMENT 'Pan Right'

`PanRightMomentary` varchar(100) DEFAULT NULL COMMENT 'Pan Right Momentary'

`panLeft` varchar(100) DEFAULT NULL COMMENT 'Pan Left'

`panLeftMomentary` varchar(100) DEFAULT NULL COMMENT 'Pan Left Momentary'

`panStop` varchar(100) DEFAULT NULL COMMENT 'Stop Panning'

`tiltUp` varchar(100) DEFAULT NULL COMMENT 'Titl Up'

`tiltUpMomentary` varchar(100) DEFAULT NULL COMMENT 'Tilt Up Momentary'

`tiltDown` varchar(100) DEFAULT NULL COMMENT 'Tilt Down'

`tiltDownMomentary` varchar(100) DEFAULT NULL COMMENT 'Tilt Down Momentary'

`tiltStop` varchar(100) DEFAULT NULL COMMENT 'Stop Tilting'

`irisAuto` varchar(100) DEFAULT NULL COMMENT 'Automatically adjust the iris'

`focusAuto` varchar(100) DEFAULT NULL COMMENT 'Automatically adjust the focus'

`backLightOff` varchar(100) DEFAULT NULL

`shutter` varchar(100) DEFAULT NULL

`autoPan` varchar(100) DEFAULT NULL COMMENT 'Automatically Pan the Camera'

`manualIrisToggleLatch` varchar(100) DEFAULT NULL

`whiteBalance` varchar(100) DEFAULT NULL

`IDDisplayEnable` varchar(100) DEFAULT NULL

```
`IDDisplayTop` varchar(100) DEFAULT NULL

`disableAlarmDisplay` varchar(100) DEFAULT NULL

`disableAlarmBlinking` varchar(100) DEFAULT NULL

`zoomWide` varchar(100) DEFAULT NULL COMMENT 'Zoom Wide'

`zoomTele` varchar(100) DEFAULT NULL COMMENT 'Zoom Tele'

`zoomIn` varchar(100) DEFAULT NULL COMMENT 'Zoom In'

`zoomOut` varchar(100) DEFAULT NULL COMMENT 'Zoom Out'

`zoomStop` varchar(100) DEFAULT NULL COMMENT 'Stop Zooming'

`zoomStopMomentory` varchar(100) DEFAULT NULL COMMENT 'Stop Zooming

        momentary'

`irisOpen` varchar(100) DEFAULT NULL COMMENT 'Iris Open'

`irisClose` varchar(100) DEFAULT NULL COMMENT 'Iris Close'

`irisStop` varchar(100) DEFAULT NULL COMMENT 'Iris Stop'

`focusFar` varchar(100) DEFAULT NULL COMMENT 'Focus Far'

`focusNear` varchar(100) DEFAULT NULL COMMENT 'Focus Near'

`focusStop` varchar(100) DEFAULT NULL COMMENT 'Stop Focusing'

`focusManual` varchar(100) DEFAULT NULL COMMENT 'Manual Focus'

`programPresetsHome` varchar(100) DEFAULT NULL COMMENT 'Define the home preset'

`gotoPresetHome` varchar(100) DEFAULT NULL COMMENT 'Go to home preset'

`programPresetPosition` varchar(100) DEFAULT NULL COMMENT 'Define a preset'

`gotoPresetPosition` varchar(100) DEFAULT NULL COMMENT 'Go to Preset'

`clearProgramPreset` varchar(100) DEFAULT NULL
```

`location` database

`locID` varchar(10) NOT NULL COMMENT 'Location ID'

`camID` varchar(10) NOT NULL COMMENT 'Camera ID'

`recordTime` datetime DEFAULT NULL COMMENT 'Date and Time of the record'

`locLong` double DEFAULT NULL COMMENT 'Location Longitude'

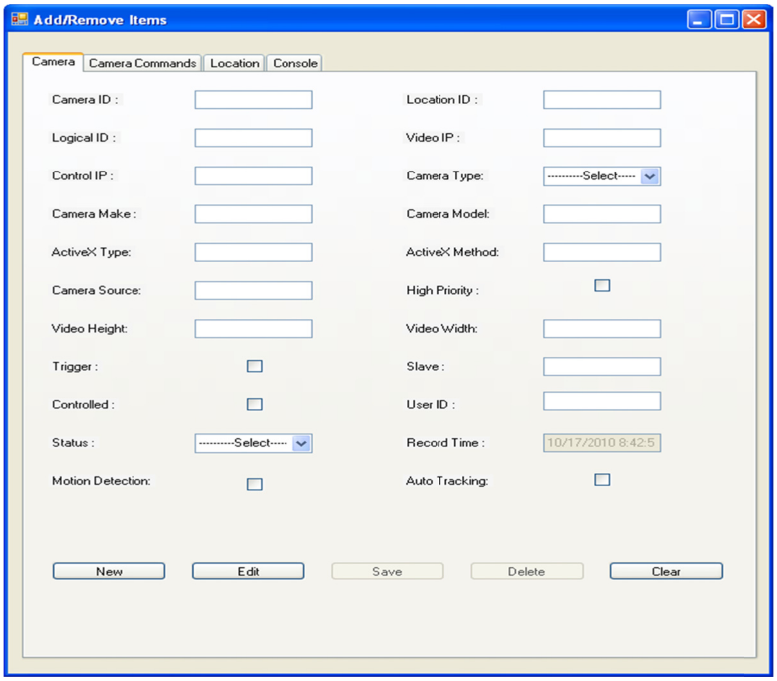
`locLat` double DEFAULT NULL COMMENT 'Location latitude'

`presetsArraySize` int(100) DEFAULT NULL

`presetsArray` varchar(100) DEFAULT NULL

Several GUIs were developed to allow the system to be updated without having to use the native database language, SQL.

To update camera information in the system database, the Camera Add/Remove GUI (Figure 8-2) is used to enter general information including an ActiveX control module name. Figure 8-3 is the GUI used to enter camera commands that the system can use to concatenate these strings with control strings to make commands to send to the camera. Figure 8-4 is the GUI to enter information about the camera location including latitude and longitude for the MapServer software to accurately place the ICON on the console map.



Record Time : 10/17/2010 8:42:5

Figure 8-2. GUI to add a camera to the system database.

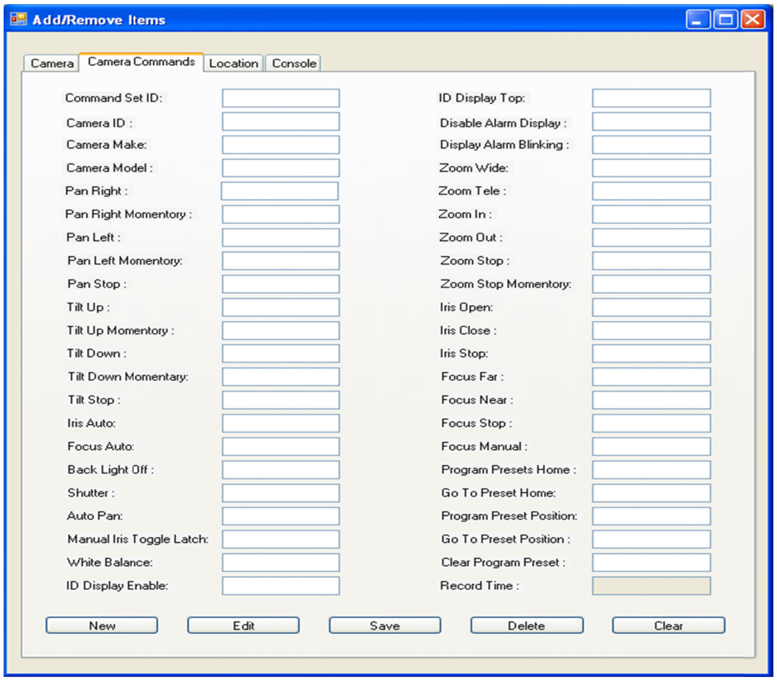


Figure 8-3. GUI to add a camera control set to the system database.

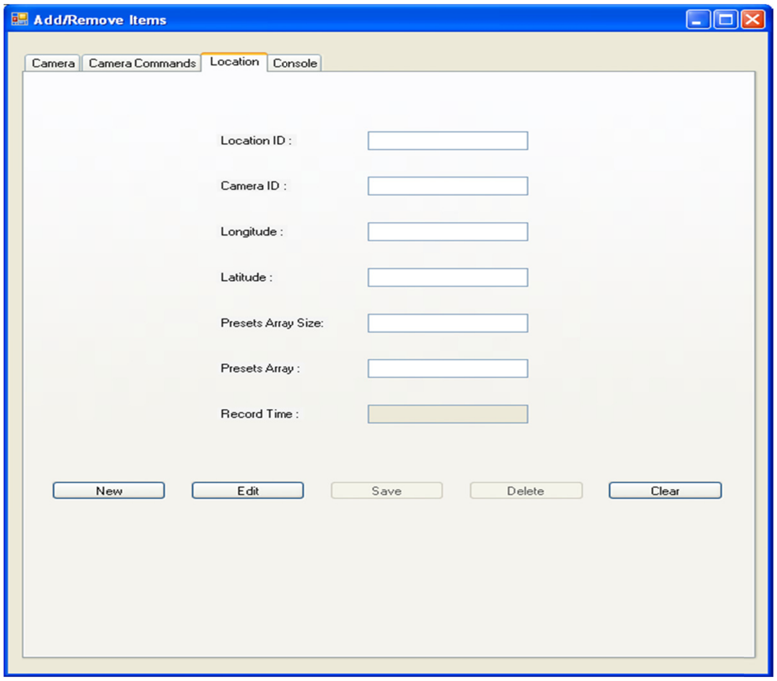


Figure 8-4. GUI to add location information to a camera in system database.

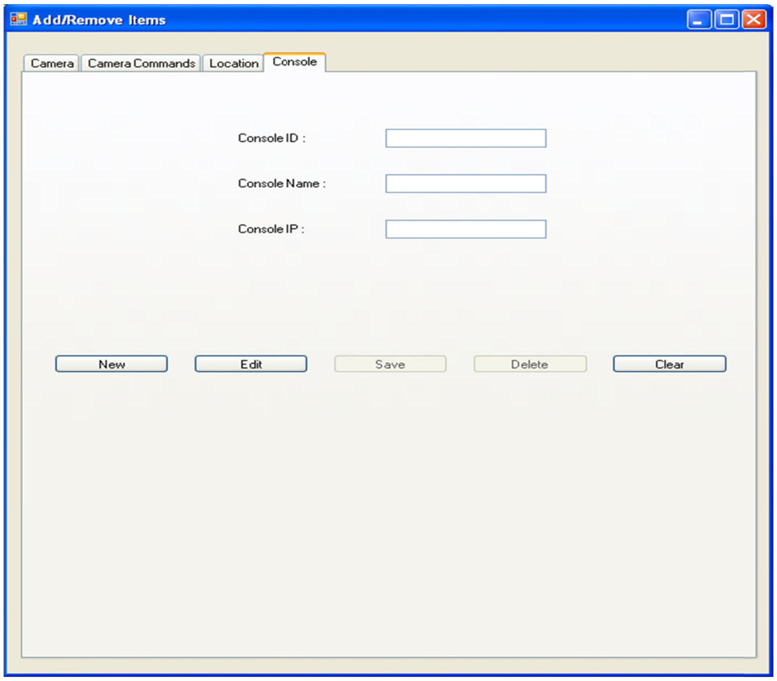


Figure 8-5. GUI to add a security control console to the system database.

Figure 8-6 shows a generic camera control GUI that was developed to control any make of camera. The camera control commands are built from data retrieved from the command_set database and concatenated with control strings to form commands that are sent directly to the camera.

By having each console act as a standalone console, this integrated and distributed system can lead to issues maintaining the integrity of the data in the databases. In order to help control the integrity of the system, a message queue service is employed (Figure 8-7).

Each time an operator takes an action, a record of that action is stored in the database and stamped with a time and a date. Each time the database is updated, the record in the database that is updated, is also stamped with a time and a date. All these updates are also distributed to all other users through this message queue. If a console is off-line or not otherwise contactable, the messages are queued until they are able to be sent. If a console has been off-line, the potential of receiving stale messages exists, and this is accommodated by checking the time and date stamp to ensure stale data in not acted upon in the database.

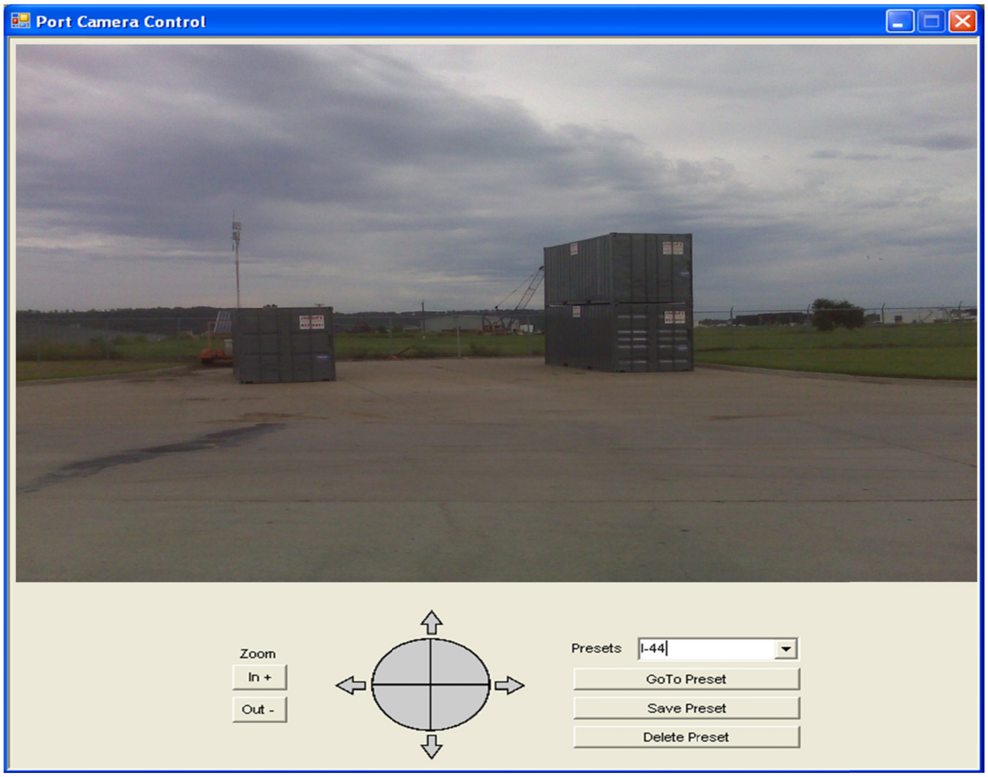


Figure 8-6. Generic camera control GUI.

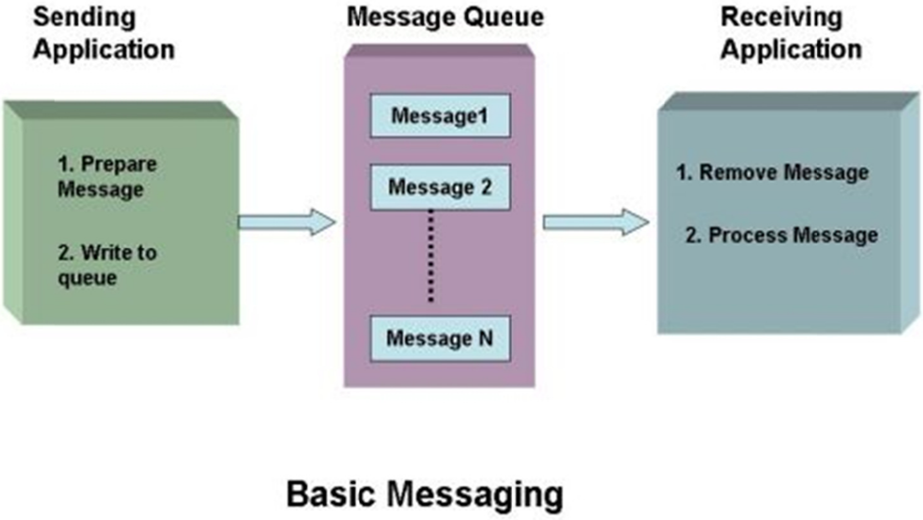


Figure 8-7. System message queue flow diagram.

Chapter 9 - Hardware Design

This research and the ICFS project in general demonstrated the use of off-the-shelf equipment to enhance port security. In Phase I, current security measures at other shipping ports were investigated and systems and sub-systems were identified where improvements could be made.

During Phase II, a demonstration of an off-the-shelf aerial surveillance vehicle, the AutoCopter from Neural Robotics. Inc. (Figure 9-1) was successfully flown. The AutoCopter was flown in the semi-autonomous mode and provided streaming video through the wireless mesh network of STRIX™ nodes back to the demonstration area and displayed at the Port Headquarters and demonstration area. Once the AutoCopter was running, pre-programmed waypoints guided it from liftoff, through the demonstration area, and back to a successful landing. Other project teams demonstrated wireless sensors and container tracking devices which also provided their data to the demonstration area through the STRIX™ wireless mesh network.

The wireless network was a set of access points with an IEEE-802.11A back-haul capability running at 54 Mbps. One of the nodes was placed on a trailer that was provided by ODOT for this project (Figure 9-2). The trailer power was generated from solar panels that kept a set of batteries charged. Through an inverter/charger, the batteries provided all power needs of the demonstration equipment for all the groups.

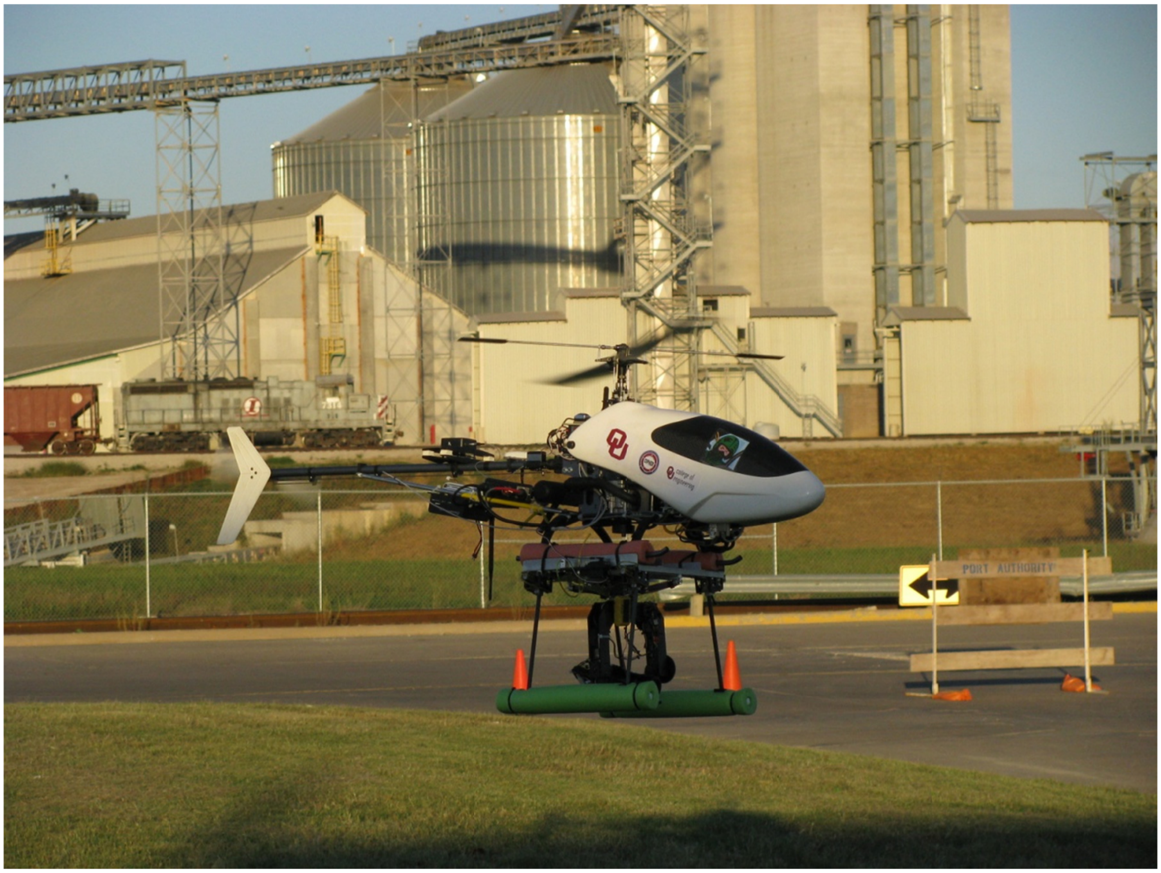


Figure 9-1. The Aerial Surveillance Vehicle hovering at the Port of Catoosa.

Other network nodes were intalled at the Dock area on the roof, as shown in Figure 9-3, the card gate location shown in Figure 9-4, and at the Port Headquarters building shown in Figure 9-5. The network provided streaming video and data to areas around the nodes from their IEEE-802.11G radios.

A mobile video feed was tested by installing a camera on a trailer and towing the trailer from the demonstration area to the main dock area, a distance of 0.75 miles (1.2

km). The data stream was successfully handed over from the demonstration area node to the main dock node without interruption to the video signal using the IEEE-802.11G network.

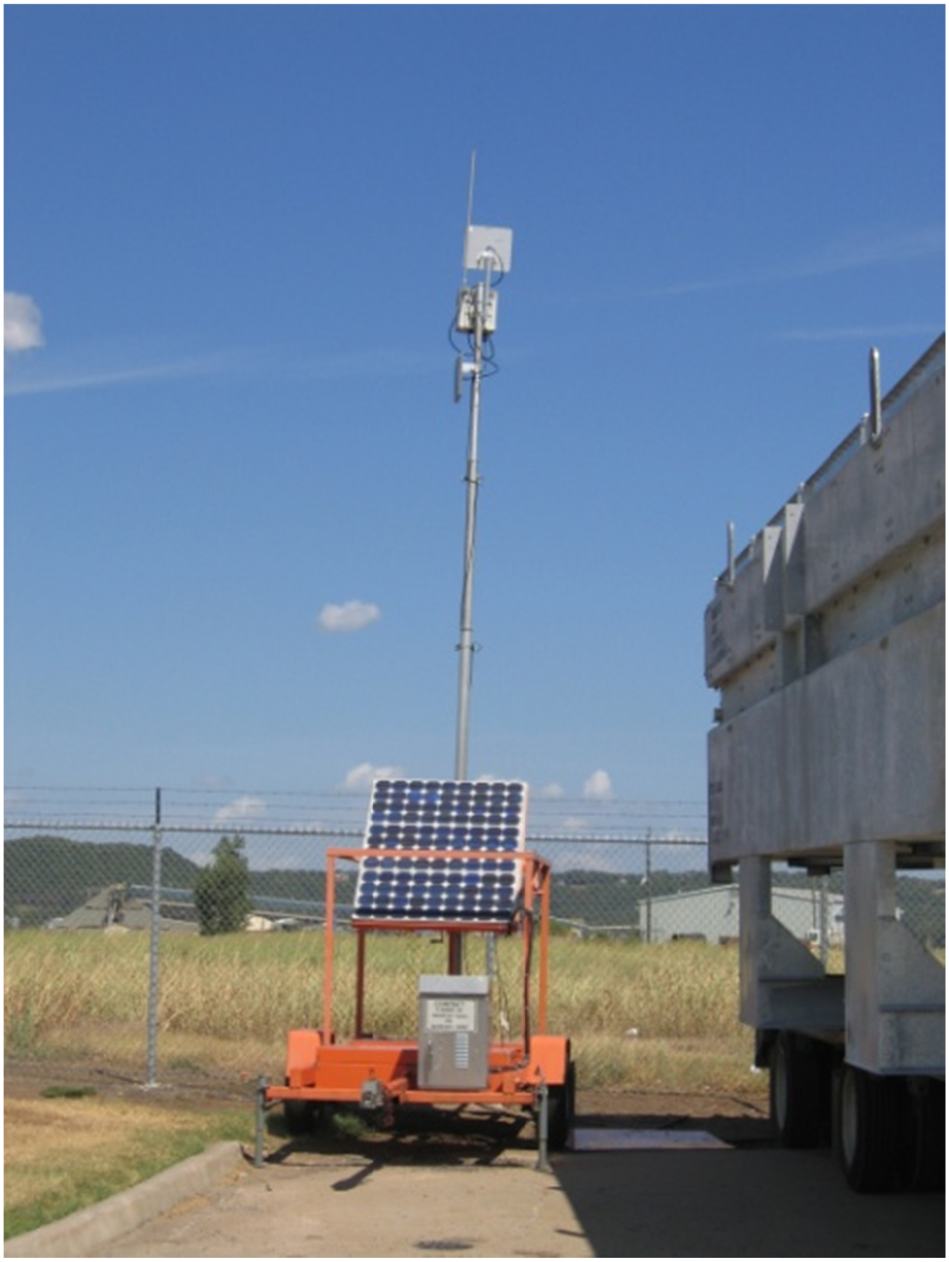


Figure 9-2. STRIX™ wireless network node mounted on ODOT provided trailer.

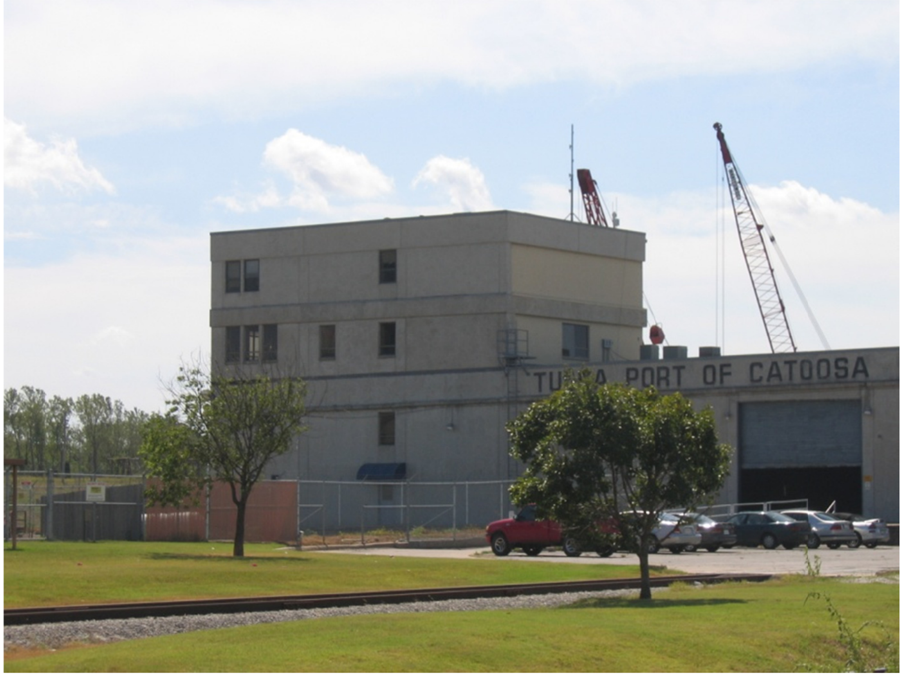


Figure 9-3. The main dock area with network node on roof.

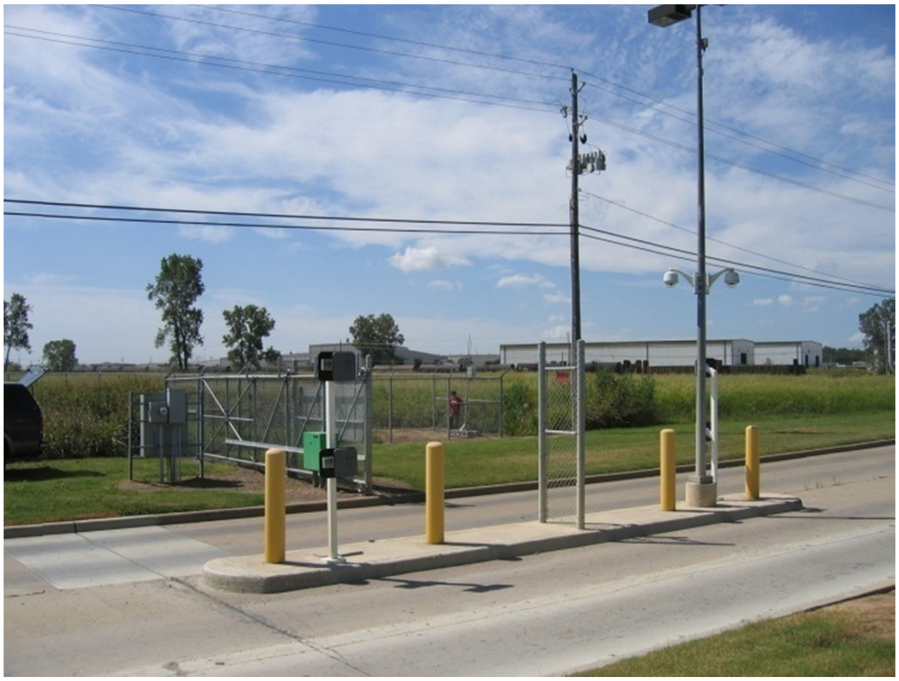


Figure 9-4. The card gate location with network node in the background.

Figure 9-5. The Port Headquarters building with network node on the roof.

During Phase III of the project, a fully operationally system, representing different building blocks was deployed at the Port of Catoosa. This system was comprised of two (2) operator consoles, one (1) with regular computer monitors and one (1) with four (4) - 40 inch displays (Figure 9-6), three (3) STRIX ™ network nodes, two (2) pan/tilt/zoom cameras, and four (4) fixed IP cameras.

The operator consoles were installed in the Port Headquarters building, one (1) in the Port Director's office and one (1) in the Security office. One (1) of the PTZ cameras and two (2) of the fixed IP cameras were installed on the roof of the Port Terminal building with a STRIX ™ network node link back to the Port Headquarters building. The second PTZ camera was installed at a newly constructed shed at the mouth of the shipping channel coming into the port (Figure 9-7). This location is ideal for a PTZ camera utilizing motion tracking since an incoming barge can be automatically tracked as it moves into the port. Two (2) fixed IP cameras were also installed here and the third STRIX ™ network node link back to the Port Terminal.

The STRIX ™ network nodes are equipped with an IEEE-802.11G radio which allows port personnel access to the network with their laptop computers while in range of the radio.

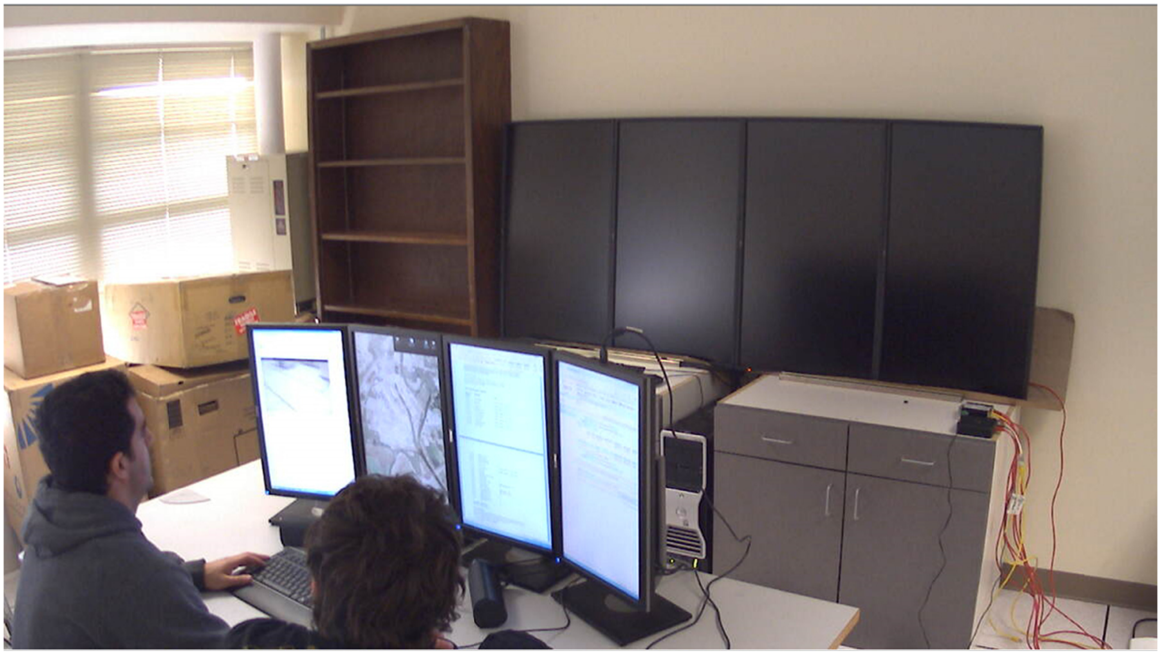


Figure 9-6. The operator console in the foreground, and the virtual management console in the background.

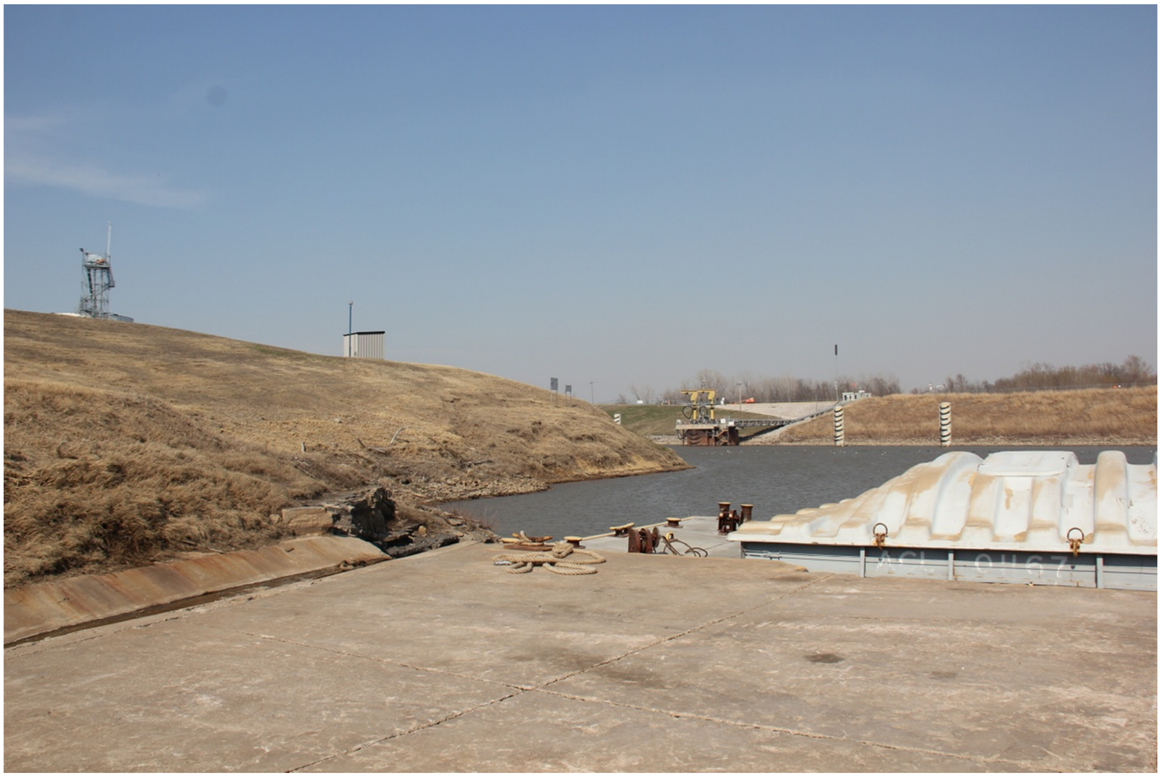


Figure 9-7. Location of the PTZ camera installation at the entrance to the port.

Two (2) types of STRIX ™ network nodes were used. An Access/One Outdoor Wireless System (OWS) 2400 (Figure 9-8), containing two (2) IEEE-802.11A radios and one (1) IEEE-802.11G radio, and an Access/One® Mobile Wireless System (MWS) 100 end point (Figure 9-9) containing one (1) IEEE-802.11A radios and one (1) IEEE-802.11G radio. The MWS was installed in an environmental enclosure to project the unit from the hot sun in Oklahoma.

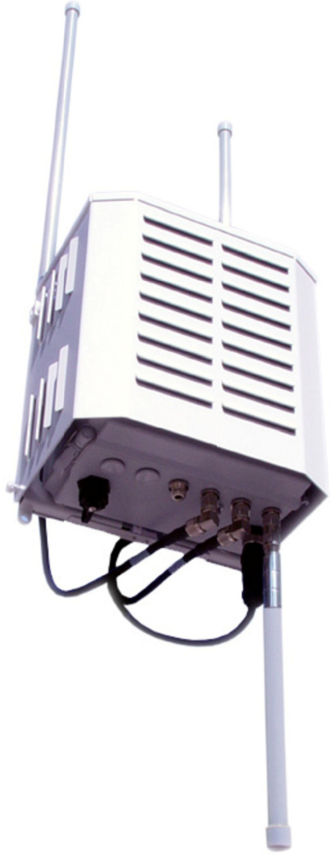


Figure 9-8. STRIX ™ Access/One Outdoor Wireless System (OWS) 2400.

(Image source - http://www.strixsystems.com/gallery-images/product-datasheets/DOWNLOAD_11.pdf)

Strix ™ Access/One Outdoor Wireless System (OWS) intelligently self-tunes, self-configures, and self-heals to optimize the overall performance and availability. The OWS architecture makes wireless broadband a full duplex technology, moving traffic more efficiently through the network and utilizing different RF frequencies and channels for network connectivity and client access.

OWS offers great scalability, efficiently and economically minimizing the number of wired termination points required in the network, greatly reducing deployment and operating costs and the Total Cost of Ownership (TCO).

Figure 9-9. STRIX™ Access/One® Mobile Wireless System (MWS) 100.

(Image source - http://www.strixsystems.com/gallery-images/product-datasheets/DOWNLOAD_27.pdf

Strix™ Systems Mobile Wireless System MWS-100 is ideally suited for mobile wireless broadband for public safety and transportation systems. The MWS delivers high-throughput and low-latency at speed for video, voice and data over mobile 802.11a/g and high-power licensed 4.9 GHz for public safety applications.

The MWS 100 is small, durable, and portable, designed for any vehicle type, enabling the longest reach and instant mesh hand-off compared to any other mobile wireless devices. Delivering seamless mobility for public safety, emergency medical, fire, industrial, mobile enterprise and many other applications, the MWS offers superior multi-megabit, multi-RF and multi-channel capabilities unique in the industry.

There were two (2) types of pan/tilt/zoom cameras deployed. The Infinova® V1750 Pressurized Dome (Figure 9-10) and the AXIS Q6032-E PTZ Dome Network Camera (Figure 9-11). The AXIS camera was equipped with a built-in video encoder and motion detection and tracking software. The AXIS camera also included an ActiveX control that was incorporated into the system software and enabled easy control of camera functions. The Infinova® camera required a separate video encoder (Figure 9-12) that also included a built-in terminal server, but no ActiveX control was provided. As such, an ActiveX control module was written in Visual Basic Plus (VB+) and this module allowed the camera to work well in the system.

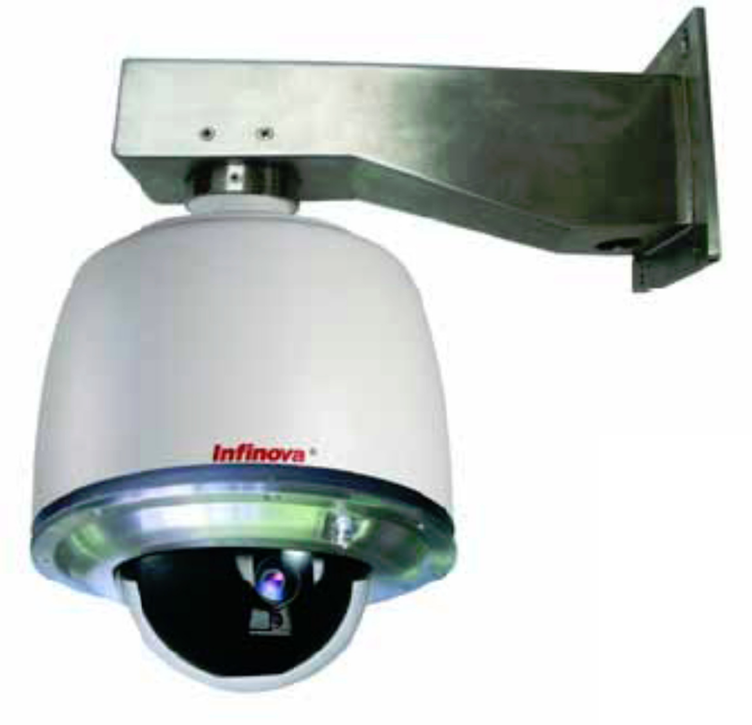


Figure 9-10. Infinova® V1750 Pressurized Dome Camera.

(Image source - http://www.infinova.com/index.php?cometo=dispro&proId=306)

Infinova's rugged V1750A series pressurized PTZ dome cameras feature a nitrogen pressurized stainless steel rim for maximum protection against airborne contaminants and moisture. Special valves minimize decrease in pressure over time. Solid-state sensors in the housing relay important system information, such as internal temperature and pressure readings, back to the control center. Non-volatile memory in the housing enables automatic downloads of camera presets and other data in the event that the camera and drive module must be replaced.

Figure 9-11. AXIS Q6032-E PTZ Dome Network Camera.

(Image source - http://www.axis.com/files/datasheet/ds_q6032_43051_en_1106_lo.pdf)

AXIS Q6032-E has a fast and precise pan/tilt response. In addition, it can tilt 20° above the horizon for a total tilt range of 220°, enabling better views, especially over uneven terrain. It has 35x optical and 12x digital zoom. License plates can be read from a distance of 160 m (525 ft.) The camera has an auto-tracking functionality that can automatically detect and follow a moving object within the camera's field of view.

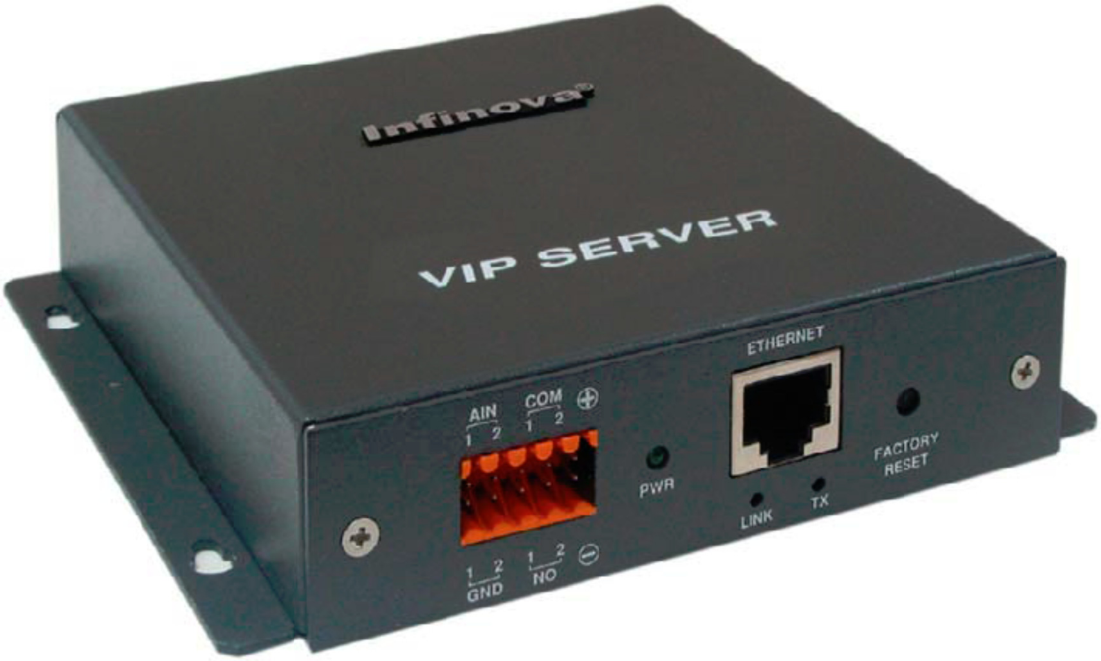


Figure 9-12. Infinova® V-2503 Video encoder and network terminal.

(Image source - http://www.infinova.com/download/company/MegapixelandIPproductfamily2011.pdf)

> The V2503-M VIP Server is a product based on MPEG-4 video encoding. The V2503-M VIP Server supports complete TCP/IP protocols, and provides network based surveillance and remote control functions. The multicasting function enables transmission of real-time video to multiple video receivers simultaneously.

Fixed cameras were installed at the Port Main Terminal and the entrance to the port waterway. These cameras are the AXIS 223M IP camera (Figure 9-13) and provide 2.0 M-pixel resolution. Environmental enclosures were used to protect the camera from the heat in Oklahoma.

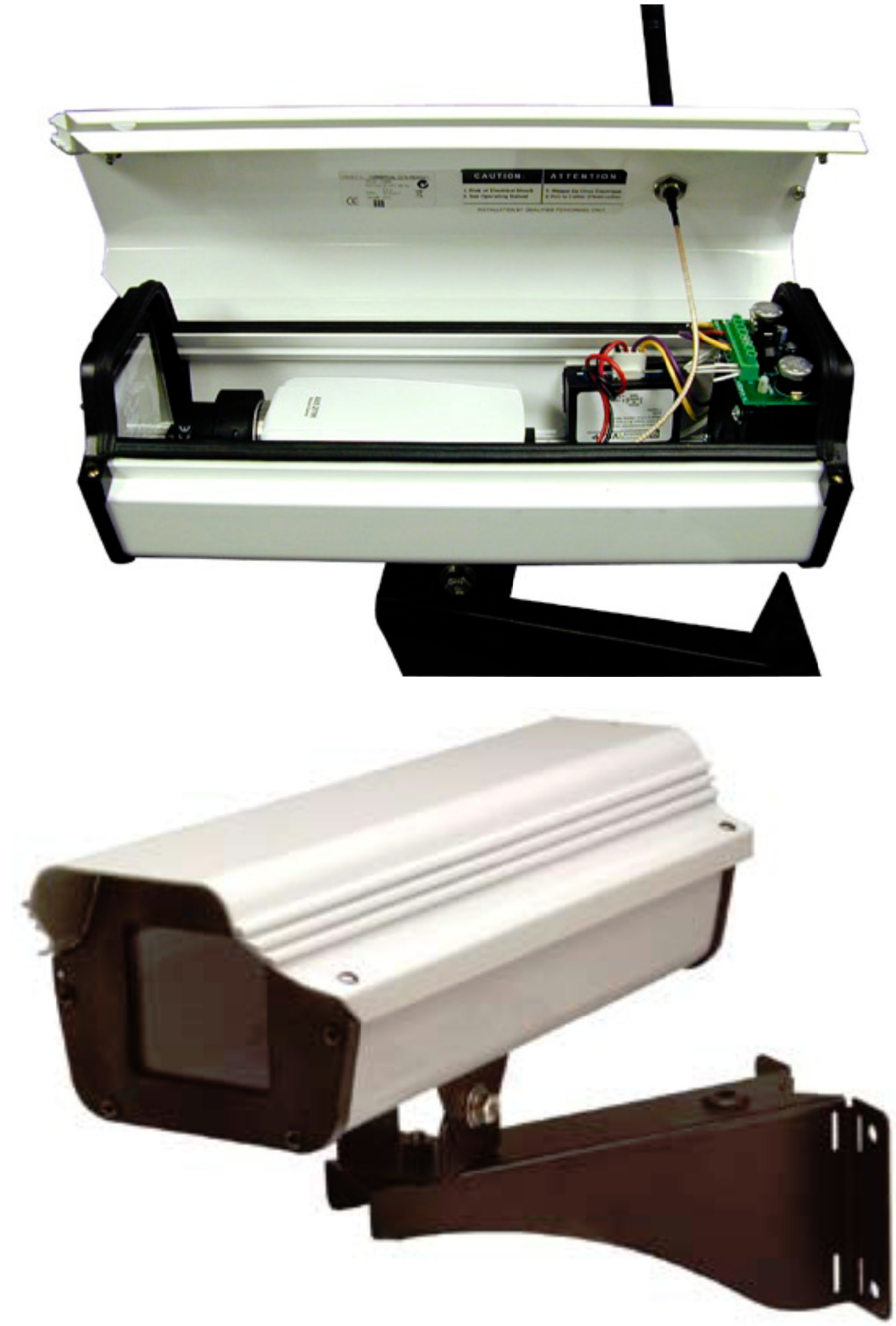


Figure 9-13. AXIS Environmental enclosure and AXIS 223M IP camera.

(Image source -
http://www.axis.com/files/datasheet/ds_211W_housing_29892_en_0709.pdf and
http://www.axis.com/files/datasheet/ds_ach13hb_25355_us_0508_lo.pdf)

> With 2 megapixel resolution, the AXIS 223M delivers crisp and clear images with exceptional image detail, perfect for the identification of individuals and objects of interest. AXIS 223M features automatic day and night functionality with removable infrared-cut filter for increased light sensitivity. Power over Ethernet (IEEE 802.3af) supplies power to the camera via the network, which eliminates the need for power cables and reduces installation costs. The two-way audio support allows remote users to listen in on an area and communicate with visitors or intruders. The powerful event management includes video motion detection, active tampering alarm, audio detection and pre-and post-alarm buffering.

In order to connect the cameras, video encoders and terminal servers to the STRIX ™ nodes, a network switch was required. Taking into account the environmental conditions and the need to power the devices out on a pole, the N-Tron 100-POE4 (Figure 9-14) Power-Over-Ethernet (POE) temperature hardened Ethernet switch was used. This switch provided four (4) 100 Mb POE ports and four (4) additional 100 Mb ports to connect the system devices. By using a POE switch, power to the camera was provided over the Cat-5E network cable and an additional power cable was not required to be run up the pole to the device.

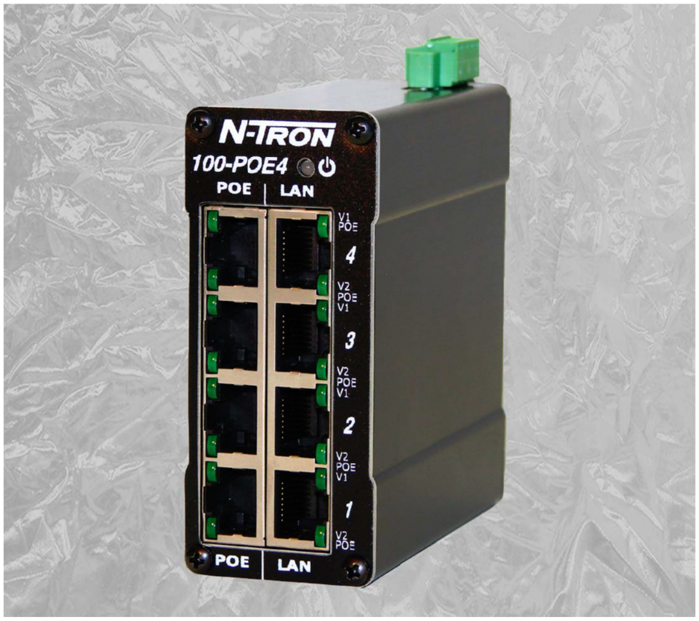


Figure 9-14. N-Tron 100 Mb PoE switch.

(Image source - http://www.n-tron.com/store/index.php?main_page=product_info&cPath=1&products_id=137)

> N-TRON's Industrial Power over Ethernet (iPoE) is designed to transmit power, along with data, over an Ethernet network and is ideal for PoE capable devices where running an AC power feed is either not possible or cost effective. This feature allows an end-user to power a PoE camera, wireless access point, or any other PoE capable device without the need for running separate wires for power.

With all system device installations, electrical power must be considered. Although commercial line power was provided to the equipment locations, facility power at the Port of Catoosa has been known to fluctuate. To preclude the power interruptions from bringing down the system during short facility power outages, back-up power is installed at the camera locations. The back-up power consists of a Tripp Lite

PowerVerter APS 1250W Inverter (Figure 9-15) and two (2) Optima Model D31M Blue Top Batteries (Figure 9-16).

The batteries are charged by the inverter charge controller from facility power. The inverter provided system power to the equipment from the batteries directly, not from facility power. This 'on-line' mode supplies un-interrupted power to the system equipment preventing switch-over interruptions when facility power drops off-line.

The cameras and network equipment can remain online through a three (3) hour power outage to provide port operators live video of the port waterway.

Figure 9-15. Tripp Lite PowerVerter APS 1250W Inverter.

(Image source - http://www.tripplite.com/shared/product-pages/en/PV1250FC.pdf)

Figure 9-16. Optima Model D31M Blue Top Battery.

(Image source - http://www.optimabatteries.com/_media/documents/specs/D31M.pdf).

The D31M is Optima's most powerful single-unit Blue Top battery. The D31M Blue Top offers exceptionally high CCA for its size and boasts 75 amp hours of current storage for long deep-cycling run times. The D31M Blue Top will not off-gas in normal operation, but for complete safety in enclosed spaces its overpressure vent will accept a remote venting tube.

Chapter 10 - Results

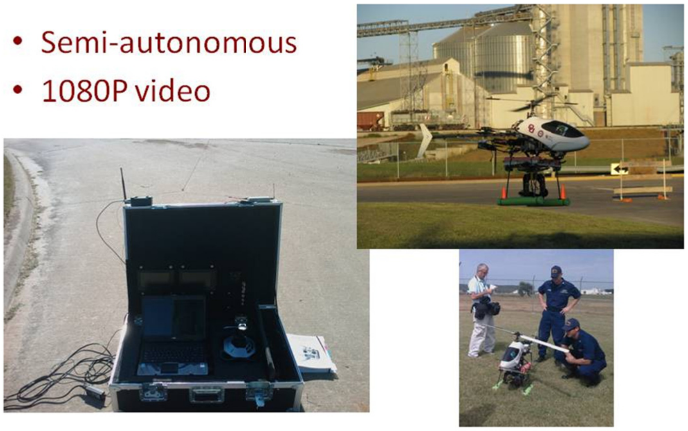
The Intermodal Containerized Freight Security research project was accomplished in three phases: 1) Research into existing technologies for container security and tracking, cargo manifesting, and port surveillance, 2) Development and testing of devices that fill in the gaps of current technologies, and 3) fielding a prototype system at the Port of Catoosa.

In Phase I, existing technologies were studied for container security, development of scenarios for Port Security using the Port of Catoosa as the model, and development of system requirements for a security system. An initial design for the hardware and testing of base-unit hardware and software, while insuring robustness of the hardware design was accomplished. Another task was to define system requirements for unmanned Aerial Surveillance Vehicle (ASV) deployment, determine requirements and metrics for demonstration, identify dependencies, and develop contingency plans. The development of two representative scenarios for the demonstration of surface and air surveillance of the port was accomplished.

During Phase II, development of a detailed design for the ASV (Figure 10-1) hardware and software modules: the selection of ASV components, coordination and control of ASV teams, integration of the instrumentation payload, test procedures and fail-safe operations were completed [7]. It was determined that COTS hardware was available for the ASV (Figure 10-2). In addition, a Ground Control System (GCS) capable of mission planning and resource deployment was developed to implement the scenarios identified. The GCS used waypoints, altitude, and attitude information as appropriate to deploy and control the ASV system. Mission planning was accomplished using existing map/satellite/aerial images and the mission was uploaded to the ASV via the wireless data link. The ASV proceeded along the planned route and returned with minimal operator intervention. The loss of instrumentation or communications, and other safety issues were addressed in the development of the GCS.

The Ground Control Station sends waypoint information to the Aerial Surveillance Vehicle via a data modem for autonomous flight. Flight commands (Pitch, Roll, and Yaw) can also be sent via the data modem in the semi-autonomous flight mode. Video is transmitted to the Ground Control Station from a video transmitter on the Aerial Surveillance Vehicle then encoded and made available for dissemination on the local area network.

Wireless network equipment was deployed around the port to test and demonstrate the capabilities of systems that were proposed. These systems provided video feeds from mobile cameras, fixed cameras, and ASV/GSV mounted cameras. These video streams were sent to the port headquarters building, as well as the demonstration area and container storage location. Other team members demonstrated integrated sensor units with COTS hardware and developed software for the TinyOS environment using nesC and the data from these sensors was sent over the installed



- Semi-autonomous
- 1080P video

Figure 10-1. Aerial Surveillance Vehicle and Ground Control Station.

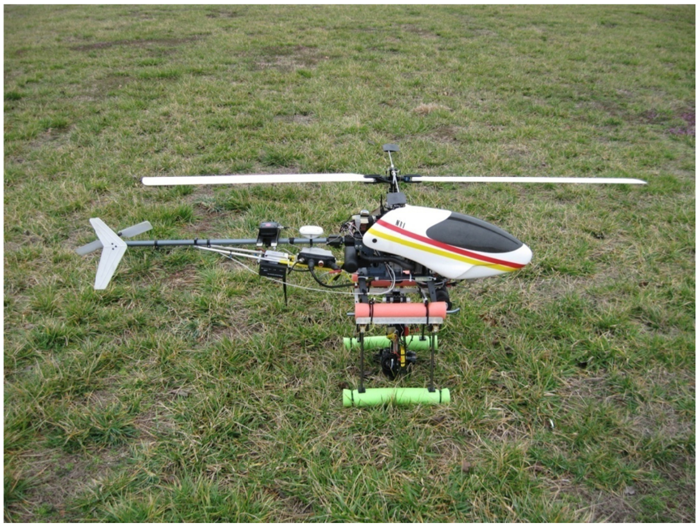


Figure 10-2. The Aerial Surveillance Vehicle used for the demo project.

A Vario Benzine trainer equipped with Global Positioning System, Altitude and Heading Reference System, and Camera Gimbal. Operational parameters of the ASV, including their altitude, attitude, and velocity were relayed to the GCS via the wireless data link and displayed in real-time using the visualization component of the GCS.

wireless network. In addition, the integration of sensor suites and field testing for robustness and safety of the applications were accomplished. This design consisted of a sensor base unit that can communicate with a variety of sensors, pickup RFID tag information, collect GPS information, and communicate by wireless means with other wireless units.

Containers were placed in two representative configurations: single container and stacked containers. Containers were instrumented with RFID devices that keep track of container inventory. As boxes with RFID labels were loaded, the container inventory was updated into a central database. If boxes were removed, the database reflected these changes also. Additional sensors for temperature, vibration, light, and door opening were also tested. This information was transmitted to the control console over the wireless network and, if recalled, displayed on the screen. If unauthorized container opening was detected, an alert was displayed on the control console [34]. A test at the Port of Catoosa using one ASV, one GSV, and a set of containers with sensor and communications instruments was accomplished with favorable results [7].

Phase III of the project was to install a prototype system at the Port-of-Catoosa and demonstrate the functionality of the systems. During this phase a prototype demonstration using COTS technology and custom software was accomplished. Field testing of hardware and software configurations in a variety of settings and conditions was also demonstrated.

Again, based on work from the development of a Statewide Intelligent Transportation System [5], a simplified approach to system integration is demonstrated. This ITS work has continued to be enhanced over the years with little change to the architectural foundation, demonstrating the robustness of the concept [30]. The 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 control center and does not require any specialized equipment. Any single instance of the ITS Console is capable of functioning independently as a control center for the entire State. However, a unique aspect of this architecture is that a large number of these low-cost consoles can be deployed to operate simultaneously in a fault tolerant peer-to-peer network.

For the port project, 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, to avoid costly and recurrent software licensing fees [31]. 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, www.mapserver.org). 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 video, of controlling the PTZ cameras, and of controlling, configuring, and acquiring data from 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.

The software architecture, shown in Figure 10-3, is similar to the Intelligent Transportation System mentioned in [5]. The database includes tables that contain all the necessary system information. Tables for the devices, device locations, device command sets and sensor data sets are created to include all data vital for the overall system. The database interfaces with the application software by an Open Data Base Connectivity

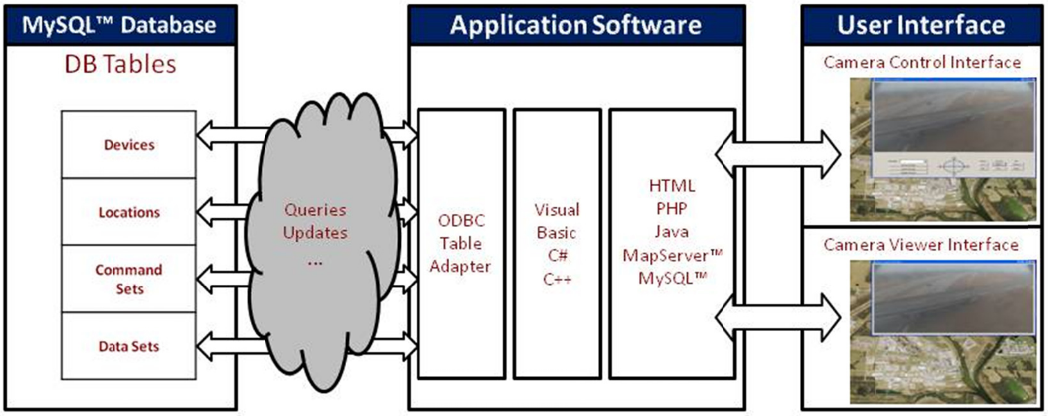


Figure 10-3. Overall software architecture.

> Commercial-off-the-shelf software is used to reduce operation and deployment costs. (Apache, MySQL, and MapServer) MSMQ is used to coordinate and synchronize the consoles.

(ODBC) table adapter. This table adapter carries all the queries and updates back and forth from the database to the application.

On the application side, several programming languages are used to interoperate with the system database and the user interface. For example, VB.NET is used to create the "Camera Viewer" which is a graphical user interface that gives the console operator access to the live video feed of a camera situated at the port. Another example is using PHP script to link the MapServer application to the database and web server. The dynamic web interface that shows the map of the Port of Catoosa is created using PHP script. On this interface, the user will be able to choose from and view different live video feeds at different locations. The use of various programming languages gives more freedom for the developers to choose the best language to fit the task in hand. The last part of the software architecture is the user interface. This interface allows the user to view and control any of the devices. There are two types of users: limited access user and advanced user. Limited access users are only allowed to view and request results. Whether a video stream, or the results of a database query. Advanced users can view, update, and modify all of the system's data sets in addition to the functions of a limited user.

The overall architecture of the software hosts various applications that can run on any console. The only requirement for the console to execute the application command is to be connected to the network. The surveillance system is interconnected and can be accessed by authorized personnel from any console. This network connection provides users the capability to monitor and configure all of the sensors and devices present at the port. As shown in Figure 10-4, the application handles two types of inputs: a triggered event and a user request. A triggered event is executed whenever an alert is triggered. Alerts can be the result of an out of limit sensor reading, motion detection, etc. A user request is generated through the user interface. Commands based on user inputs or triggered events are handled by the processor. For example, if a command is sent by the user to tilt camera 2, then the application receives that command and queries the database to get the specified command for that camera. The application then sends the command to camera 2. Some of the messages received by the console are update messages, in this case, the console only updates the database with no further action taken. If the request includes displaying results, such as a live video feed, the console first finds which device to interrogate by querying the database. Then, the console sends a command to the device to retrieve the required information and finally display it to the user.

The application is designed to serve different makes and models of sensors and devices. By design, adding new equipment to the overall system should not be a burdensome task. The application requires a few updates to the database and no addition to the main code.

The application software contains an interactive web interface supported by an Apache web server. The application provides the user with a map of the port and several optional features. On the map, the user can find the locations of cameras and view live video feeds from each. With adequate privileges, the user can view and control the cameras. Upon selection, the user can control a PTZ camera, for example, and be able to set different parameters for a better use of the camera.

The user will be able to move the cameras to any desired location. The user can also select different layers to add to the map, which include: control areas, roads, streams, city outlines and lakes and rivers. Adding these layers facilitates the viewing of several regions of the port. A map legend is present to quickly redirect the user to the port location in case they shift to another area on the map.

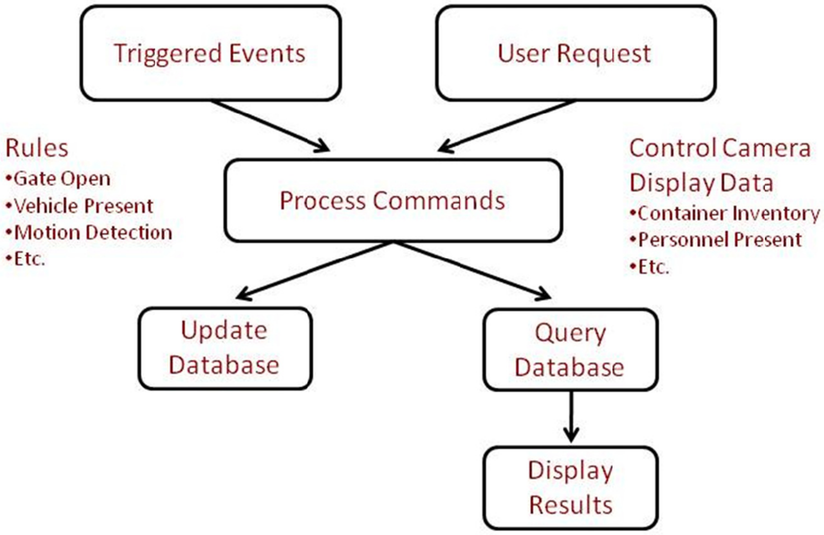


Figure 10-4. A flow diagram of the system application.

All the information present on the map is stored in the database, as well as all the changes that are sent as updates to the data tables. The database also contains locations of the cameras and sensors, and sensor data, such as alerts, activities and inventories. When an alarm goes off, the user is alerted and the database is updated accordingly. User inputs generate commands that are sent through the network. These commands are also stored in the database.

The overall system is built to facilitate interoperability among different kinds of equipment. One example of interoperability is the use of different makes and types of cameras. The system is capable of easily adding new models of cameras and integrating them to function as desired.

Currently, two types of cameras are in use at the port (Figure 10-5): fixed cameras and PTZ (Pan/Tilt/Zoom) cameras. The fixed cameras are split into two categories: those with motion detection and those without. Motion detection is considered as a triggered event that interrupts ongoing system processes. Alarms coming from static cameras are also used to direct PTZ cameras to the desired locations so that the user can then monitor and control the PTZ as required.

The PTZ cameras are also capable of performing motion detection and tracking in either of these cases: an event triggered by a fixed camera or motion detection in the surveillance area. The operator's console shows all feeds from the fixed and PTZ cameras. The operator can then subjectively analyze the live video. The system automatically triggers alarms upon motion detection and thus can alert the operator of any suspicious acts.

The idea of motion detection and tracking can be expanded into recognizing the moving objects. A study into the process of performing accurate human detection and tracking at a port is being conducted by others and is not part of this research. This study, A Personnel Detection Algorithm for an Intermodal Maritime Application of ITS Technology for Security at Port Facilities [32] will enable detection of unauthorized personnel in the secure area. It will also give the system a more intelligent aspect in finding unwanted people.

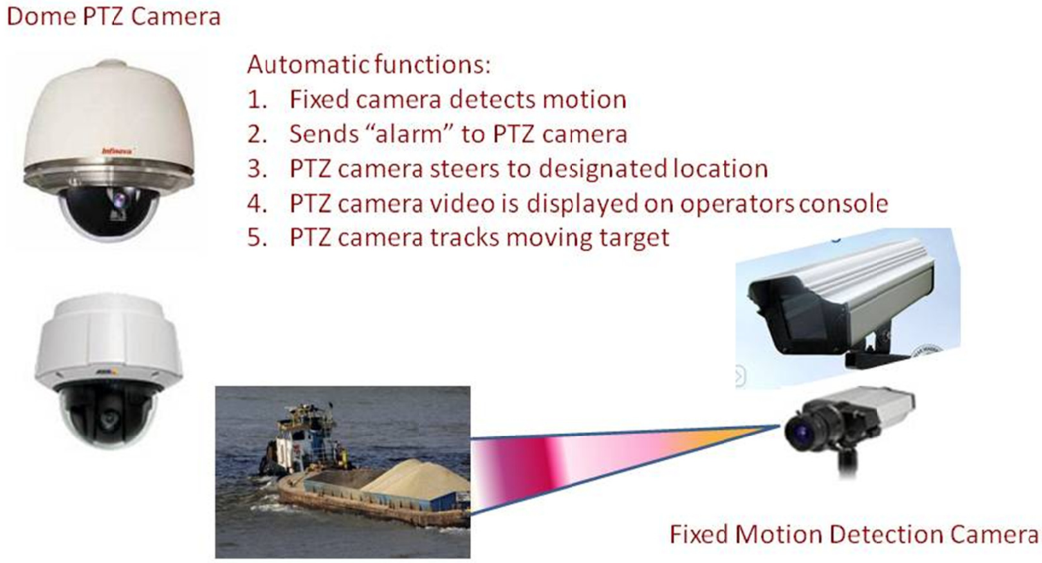

Dome PTZ Camera
Automatic functions:
1. Fixed camera detects motion
2. Sends "alarm" to PTZ camera
3. PTZ camera steers to designated location
4. PTZ camera video is displayed on operators console
5. PTZ camera tracks moving target
Fixed Motion Detection Camera

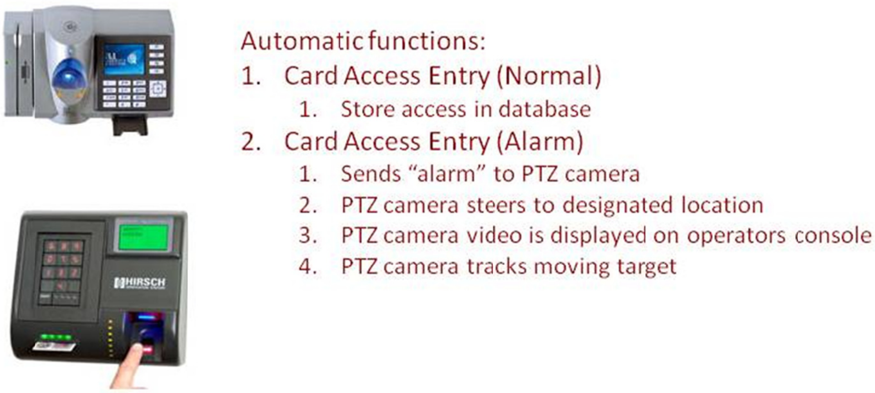
Figure 10-5. **Types of cameras deployed on the Port of Catoosa.**

Pan/Tilt/Zoom cameras were installed to give the operator control of the desired view.

One PTZ camera was equipped with motion tracking and was able to track a barge as it moved through the Port. Several fixed cameras were installed to provide video of areas of interest and as triggers for alarms based on motion detection algorithms.

Access entry equipment is present in areas where security levels are very high. Such areas, for example cargo storage areas, are under surveillance 24 hours a day / 7 days a week. Only authorized personnel are given access into and out of these areas. There are different types of devices that can be used to authorize certain individuals. Some examples are finger print access entry devices and card access entry devices. The equipment used at the port is the card access entry device that reads the electronic tag of the Transportation Workers Identification Card (TWIC) access card (Figure 10-6). Whenever an individual uses an access card, an assigned PTZ camera will move automatically to provide a live preview to the current user of that access. This helps authenticate users in a more efficient and safe way. An event of a card read by the access entry device triggers a designated PTZ camera to show the operator the detailed scene of what is happening. This easy to manage approach replaces the need to have operators perform a long subjective analysis of current video feedbacks from a variety of cameras. After moving the PTZ camera to the desired scene, the camera again takes over and starts tracking the moving targets. Unless interrupted by another user command or a higher priority alarm, the PTZ camera will keep on tracking the detected target.

Some types of the access card readers can read up to 6 inches (15.2 cm) away from its sensing area. Usually, the tag found on the access card contains a passive integrated circuit, unless the user gets close enough to be authenticated by the reader, no access is given.



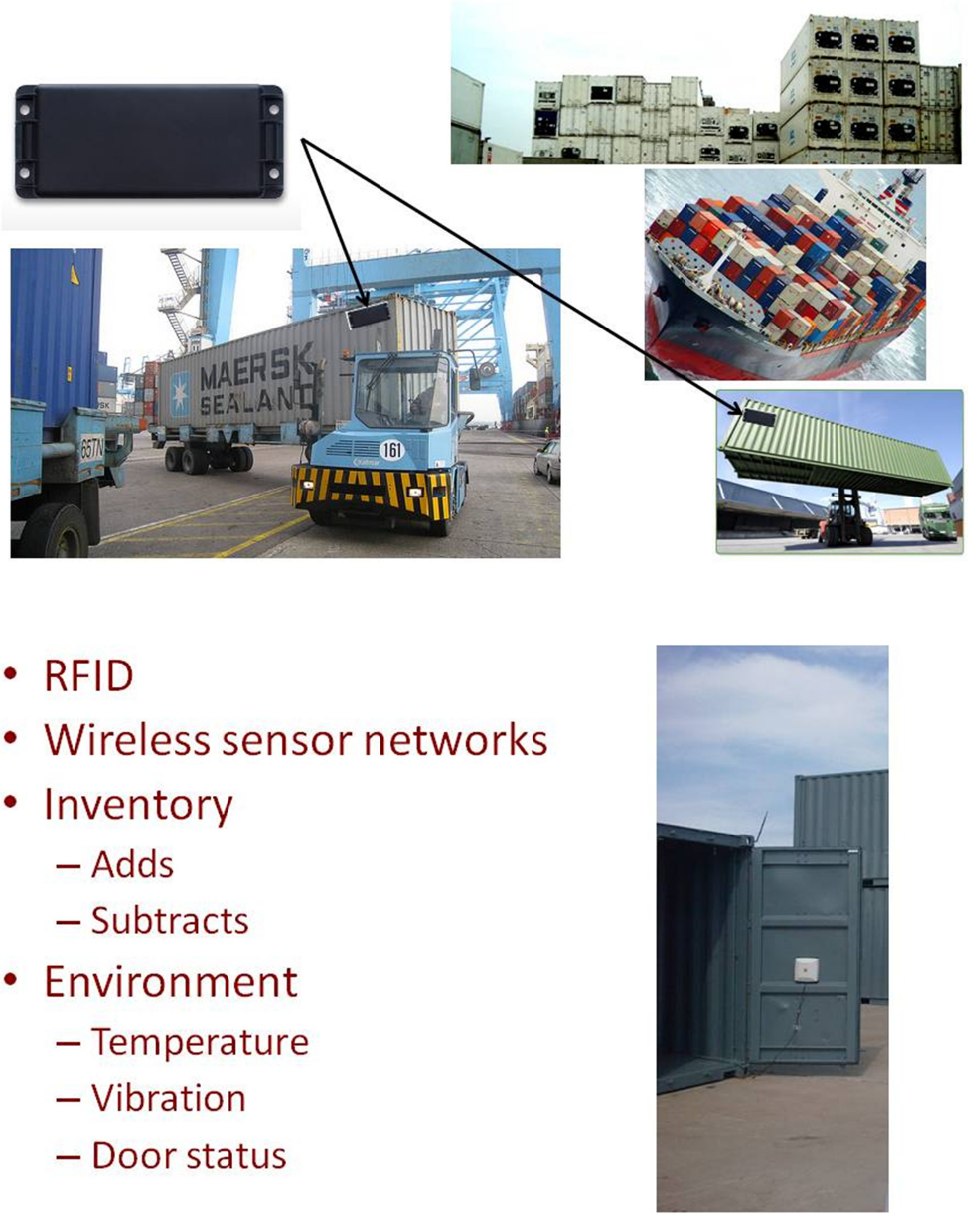
Automatic functions:

1. Card Access Entry (Normal)
   1. Store access in database
2. Card Access Entry (Alarm)
   1. Sends “alarm” to PTZ camera
   2. PTZ camera steers to designated location
   3. PTZ camera video is displayed on operators console
   4. PTZ camera tracks moving target

Figure 10-6. Type of access entry equipment that is projected to be used at the port.

While millions of containers are shipped to the United States on a yearly basis, not much information is available about each container. Attaching RFID devices, as shown in Figure 10-7, can collect sensory data about the conditions of the container, which can be very beneficial. Sensors can be used to measure humidity, temperature, light intensity, door locked/unlocked, etc.

Thresholds of these measurements are used to trigger alerts to the console. For example, a container can be carrying perishable items that require a certain range of temperature to be preserved. If the temperature, at any time, exceeds that limit, an alert will be sent out to the RFID device. This facilitates the process of keeping a suitable environment inside the container for goods safety. Door lock sensors are very important to report any alteration of the container from its source to destination. The sensors help maintain a protective environment for the contents of the container.



- RFID
- Wireless sensor networks
- Inventory
  - Adds
  - Subtracts
- Environment
  - Temperature
  - Vibration
  - Door status

Figure 10-7. Proposed wireless container tracking equipment to be attached to containers.

The bottom photo shows the actual hardware used for the Phase II demonstration at the Port of Catoosa.

Monitoring each container strengthens the container security and provides valuable information. All this data in addition to location data can then be stored in the database. As ships or barges enter the port network, the RFID devices start data transfers to the system. Information about all the containers are collected and analyzed by the console operator. The location data informs the operator of the current position of the container after it is put in a staging area at the port. Also, any relocation of the container can be monitored from the console.

The process of reading all the RFID devices from the containers can be a long process if a huge load is being carried by the ship or barge. Reading the RFID devices starts at the moment the ship/barge enters the port coverage area. From that point, until all the containers are stored, the RFID reader will have enough time to complete the process.

The architecture of the distributed IP network is shown in Figure 10-8. In addition to video streams, communications with devices, including control and data acquisition for sensors, is also performed over the 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.

Existing technology makes it extremely easy to create a fault tolerant network that can handle multiple streams of video, data, and sensor commands. Reaching locations that do not have existing communications infrastructure can be accommodated using

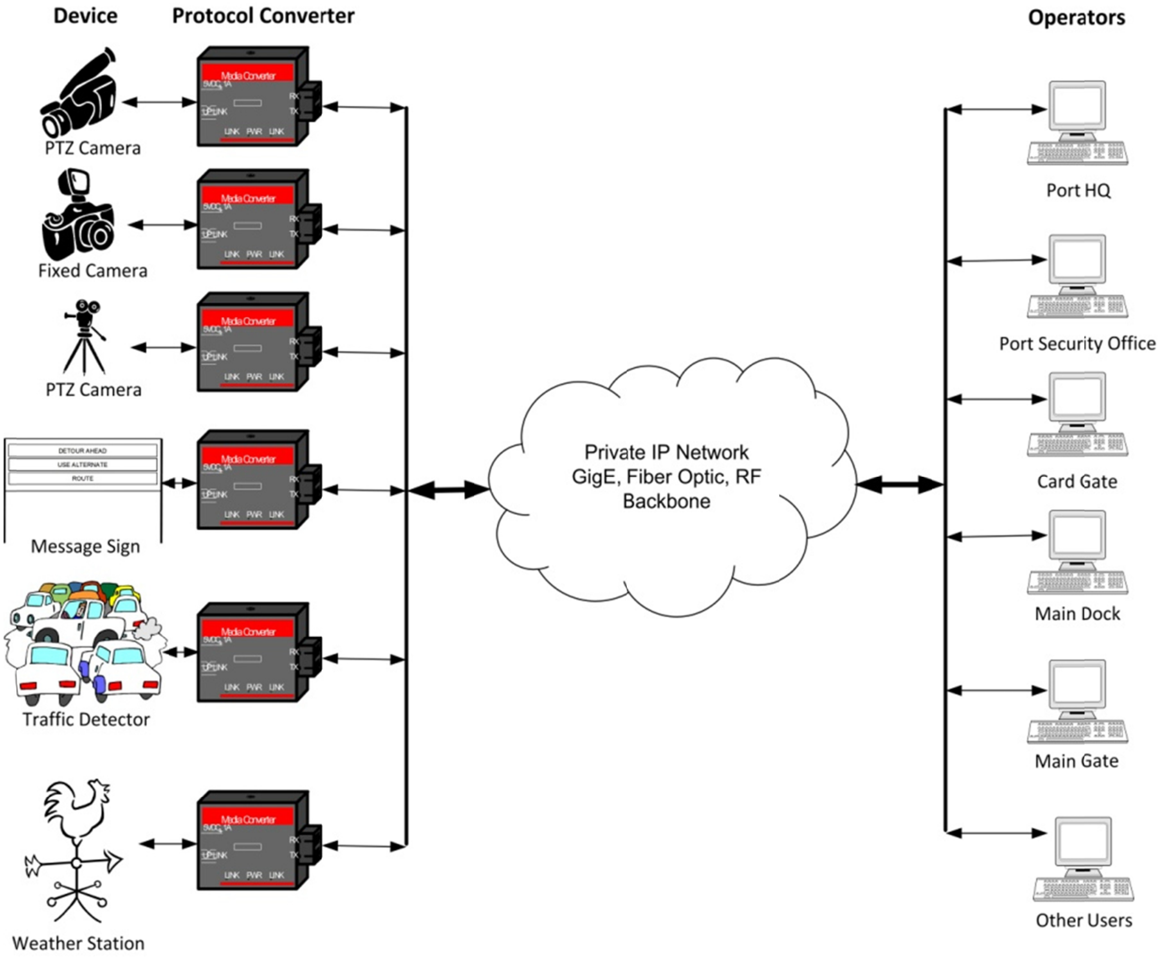
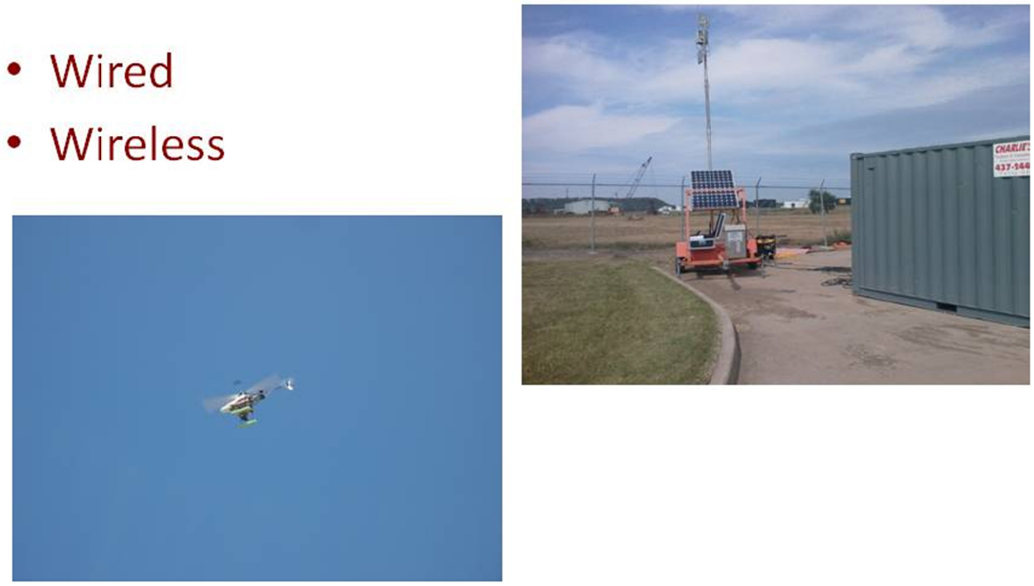


Figure 10-8. Distributed IP network architecture.

wireless access nodes, installed with high-bandwidth and encryption to accommodate the location and equipment (Figure 10-9). Careful planning can ensure redundancy in the network and, therefore, operator console access and equipment control is achieved.



- Wired
- Wireless

Figure 10-9. Wireless Video Network Link.

This network brought video from the Aerial Surveillance vehicle to the port wireless network making the video available to any console on the port.

Chapter 11 - 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 and reduce the workload.

This project demonstrated the use of off-the-shelf aerial surveillance vehicles equipped with video cameras and wireless video downlinks to provide a birds-eye view of port facilities to security control centers and security patrols on the ground to enhance existing security measures and help secure the port facilities.

The development of a structured, well designed, and simple software implementation, together with off-the-shelf technologies can be deployed, multiplied, and integrated at a minimum cost to the port facility while reducing the software maintenance costs associated with system evolution. Simple software adapters known as ActiveX controls and terminal servers to connect non-network enabled equipment and legacy equipment to the network can be used to allow integration of existing systems.

This project demonstrated a distributed architecture where each security console is stand-alone, yet integrated into the network and system.

Although only two (2) currently, the system supports many operators connected to the system without interrupting other operators. It also demonstrated many devices existing on the system, and showed that additional devices can be added by updating the database through provided Graphical User Interfaces (GUIs).

The premise of this system design was – Any operator can control any device at any time to access any information needed to accomplish their mission. Whether at the Port of Catoosa, in Washington DC, or in an Emergency Operations Center, the operator has visibility into that facility.

Port security is essential for maintaining safe and efficient movement of cargo. In these times of constrained budgets, new and innovative approaches must be considered and implemented. The Inter-modal Containerized Freight Security project has demonstrated that many existing technologies can be integrated in a cost-effective manner to provide port security. Through the use of off-the-shelf hardware and software, an innovative, low cost, and scalable security system was developed and installed at the Port of Catoosa.

The Intermodal Containerized Freight Security project was undertaken by many individuals, teams, universities, and corporations, and much good work was accomplished by all these entities. The culmination of the Phase II work was an enormously successful out brief and demonstration at the Port of Catoosa.

Bringing all these individual components and projects together, making last minute adjustments to designs, and coordinating numerous different technologies to simultaneously function in an unproven environment was a tremendous challenge.

The actual deployment of equipment: networking, camera systems, and sensors, for Phase III after all this designing, testing, and pre-staging was accomplished was simple. By using good engineering practices and management skills, the entire project succeeded.

In the future, as new technologies become available to augment freight security, whether they are new container tracking devices that can monitor the location of a container in the storage yard or track the container as it moves through the inter-modal shipping channels, these new technologies can be added to the system by simply adding them to the database and incorporating their ActiveX control.

This project was accomplished using a Systems Engineering approach. Where applicable to the stage of the project, it integrated all the disciplines and specialty groups into one team effort. By forming a well-structured process that proceeded from initial concept to deployment, this approach considered both the business and the technical needs of the customer while maintaining the goal of providing a quality product that met the users' needs.

The phases of a systems engineering approach include: Operations, Performance, Test, Manufacturing, Cost and Schedule, Training and Support, and Disposal. Because of the short nature of this research, not all phases were necessary or considered, and will be left for future work. The use of Commercial-Off-The-Shelf components greatly reduces the risks of development and manufacturing. Additionally, by supporting Plug-and-Play components, the architecture can support newer technologies to replace older and failed components.

Aerial Surveillance Vehicle

The integration of the camera gimbal and helicopter provided a stable platform for demonstration of aerial video surveillance. Frequency conflicts between the ground control station and the video down link were quickly resolved with smart channel selection. RC controller conflicts with the NovAtel GPS receiver were catastrophic until it was realized that the GPS receiver sensitivity was such that during alignment, the RC controller, operating at 72 MHz prevented the GPS receiver from finding satellites. By having the operator maintain an acceptable distance from the ASV during the alignment process, this problem was quickly resolved.

In manual flight mode, the ASV performed as expected, constant operator input was required to maintain stable flight and hover. The gyro stabilized camera gimbal compensated for most ASV flight instability and produced acceptable video quality. Camera control was accomplished by a second operator. Figure 11-1 shows still images from the camcorder during manual flight. Image quality and resolution were adequate for security personnel to identify objects and individuals in the down linked video on the monitor.

In the semi-autonomous flight mode, the ASV performed flawlessly and helicopter control from the GCS was straight forward. After arriving at the point of interest, releasing the joystick provided a stable hover through the FCS. Camera control was easily accomplished by use of the second controller while viewing the video on the GCS monitor. This video was encoded and transmitted over the wireless network and displayed at the security control center. During semi-autonomous flight, the camcorders optical zoom capability provided the ability to resolve license plate numbers, container numbers and the security personnel were able to identify personnel at the demonstration area.

Optical zoom has a negative effect by reducing the field-of-view producing the "soda straw" effect. This effect described in Kumar [20] and others, requires constant attention as objects of interest quickly move into and out of the image. Figure 11-2 shows images captured from the camcorder during semi-autonomous flight of the ASV.

Figure 11-1. **Images from the video camcorder in manual flight mode.**

Images from the camera mounted on the gimbal below the aerial surveillance vehicle. The left image is while the ASV is idling on the ground. The center image is at 60 feet (18.3 meters) and 45 degrees of down camera angle. The right image is at 60 feet (18.3 meters) and 15 degrees of down camera angle. The images are still images from the recorded video file.

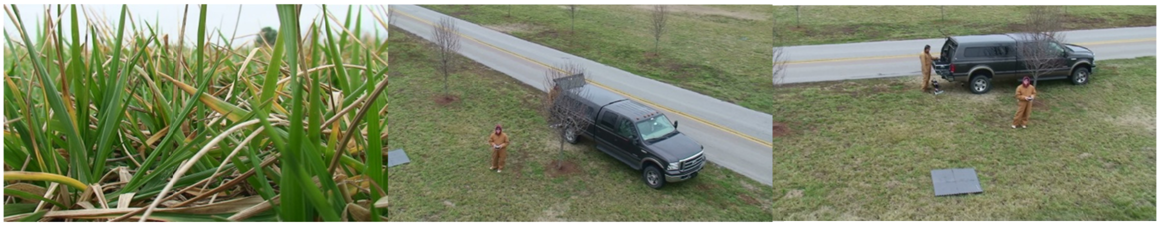


Figure 11.2. Images from the video camcorder in semi-autonomous flight mode.

Images from the camera mounted on the gimbal below the aerial surveillance vehicle. The left image is while the ASV is idling on the ground. The center image is at 40 feet (12.2 meters) and 45 degrees of down camera angle. The right image is at 30 feet (9.1 meters) and 15 degrees of down camera angle. The images are still images from the recorded video file.

Console Development

The software architecture of the ITS console has proven its robustness over the past 6 years and the overall concept, "any console, any device, any time" still holds true [30]. Additionally, the network redundancy and far reaching design is another example of good engineering leads to a good product. A few revisions in the foundation of the ITS software architecture learned over the years make the Port Security system, while basically unchanged from the ITS console, more maintainable.

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 Security Console, of displaying analog and digital video, of controlling the PTZ cameras, and of controlling, configuring, and acquiring data from RFID sensors, TWIC readers, 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 is 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 desires to take control of a certain device, the console 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 tuners connected through terminal servers. This capability provides for on-the-fly configuration of a centralized Operations Center (OC) at any given location when the need arises. Additionally, with this implementation, a remote OC can be established using wireless links if fiber or other wired networking is not available at the desired location.

The use of building blocks in hardware can also be carried over into the software as well. By creating nebulous software modules and making calls to the database for system variable names and other control module names based on user requests, additional hardware types can be added to the system without having to modify the original code. By not having to modify previous software modules, greatly reduces software maintenance tasks in the future. This also helps to maintain a common and consistent interface to the user.

Chapter 12 - Future Work

From this research, several areas still need further work to provide a more robust security system for freight movement:

- The integration of Aerial Surveillance Vehicles with their counterpart, Ground Surveillance Vehicles. This coordination should improve port surveillance and unburden port security personnel. This can save time and resources but will require much effort well beyond the scope of this work.
- As was mentioned, tracking and identification of personnel in and around the port using video detection and tracking methods. While much research has been done in this area with gait recognition, for example, this is still unproven and may require other methods that can complement it for accuracy [22].
- One area of interest is the container tagging and tracking of environmental conditions, physical location, and security information. Tracking these containers as they move around the country, outside of the port facilities, should be a high priority topic.

Bibliography

[1] Sternberg, E., and Lee, G. C., “Meeting the Challenge of Facility Protection for Homeland Security”, Journal of Homeland Security and Emergency Management, Volume 3, Issue 1, 2006, Article 11.

[2] U.S. Customs and Border Protection. Container Security Initiative Strategic Plan 2006-2010. Visited February 2010. [Online]. Available: http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/csi/csi_strategic_plan.ctt/csi_strategic_plan.pdf.

[3] “The national strategy for maritime security,” http://www.dhs.gov/xlibrary/assets/HSPD13_ MaritimeSecurityStrategy.pdf, last viewed 22 July 2008.

[4] Huck, R. C., Al Akkoumi, M. K., Herath, R. W., Sluss Jr., J. J., Radhakrishnan, S., Landers, T. L., "A demonstration of a low cost approach to security at shipping facilities and ports" in Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IX, edited by Edward M. Carapezza, Proceedings of SPIE Vol. 7666 (SPIE, Bellingham, WA 2010) 76662J.

[5] Huck, R.C.; Havlicek, J.P.; Sluss, J.J., Jr.; Stevenson, A.R.; , "A low-cost distributed control architecture for intelligent transportation systems deployment in the State of Oklahoma," Intelligent Transportation Systems, 2005. Proceedings. 2005 IEEE , vol., no., pp. 919- 924, 13-15 September 2005.

[6] “Establishment of U. S. antiterrorism maritime transportation system,” The American Journal of International Law, Vol. 98, No. 3, July 2004, pp. 588 - 590.

[7] Huck, R., Al-Akkoumi, M., Cheng, S., Sluss, Jr., J., and Landers, T., “Aerial surveillance vehicles augment security at shipping ports”, in Proceedings SPIE Europe Security and Defense, Cardiff, Wales, United Kingdom, SPIE Vol. 7112, Unmanned - Unattended Sensors and Sensor Networks V, September 15-18, 2008.

[8] A Persistent Eye on the World’s Sea Lanes. Lockheed martin Center of Innovation, Lockheed Martin Corporation. Insights, Volume 5, Number 2, Second Quarter 2008.

[9] Chen, W., Chen, P., Lee, W., and Huang, C., “Design and implementation of a real time video surveillance system with wireless sensor networks,” Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, May 2008, pp. 218 – 222

[10] Green, M. W., “The appropriate and effective use of security technologies in U. S. schools,” U. S. Department of Justice, Report NJC178265, September 1999.

[11] Chang, E., Wang, Y., and Wang, I., “Toward building a robust and intelligent video surveillance system: a case study”, 2004 IEEE International Conference on Multimedia and Expo, Volume 2, June 2004 pp. 1391 - 1394 Vol.2.

[12] Hampapur, A., “Smart video surveillance for proactive security,” IEEE Signal Processing Magazine, June 2008, pp.132 – 136.

[13] AN/SQR-17A (V2000) Acoustic Surveillance System. Visited February 2010. [Online]. Available: http://www.drs.com/Products/ANSQR17A.aspx.

[14] Varma, Y., and Tull, M., "Assessment of Container and Cargo Integrity Sensor Alternative", Intermodal Containerized Freight Security Project, Deliverable D.F.4, 2007.

[15] Sluss, Jr., J., Tull, M., Commuri, S., Huck, R., Varma, Y., Al Akkoumi, M., and Shrinivasa, R., "Tulsa Port of Catoosa - Demonstration Project", Intermodal Containerized Freight Security Project, Deliverable T.F.3, 2007.

[16] Foreign Trade: USA Imports from Germany Measured by weight (kg), Visited July 2011. [Online]. Available: http://www.worldportsource.com/trade/imports/weight/DEU.php.

[17] Port of Seattle Breaks Cargo Record in 2010, Seattle Port Authority News Release, January 18, 2011. Visited February 2011. [Online]. Available: http://www.portseattle.org/news/press/2011/01_18_2011_01.shtml

[18] Port of Long Beach Quick Facts, Visited January 2011 [Online}. http://www.polb.com/about/facts.asp.

[19] Chvatal, V., “A combinatorial theorem in plane geometry,” Journal of Combinatorial Theory, Series B, Volume 18, Issue 1, Pages 39-41, February 1975.

[20] Kumar, R., Sawhney, H., Samarasekera, S., Hsu, S., Tao H., Guo, Y., Hanna, K., Pope, A., Wildes, R., Hirvonen, D., Hansen, M., and Burt, P., “Aerial video surveillance and exploitation,” Proceedings of the IEEE, Volume: 89, Issue: 10, Oct 2001, pp. 1518-1539.

[21] Brakman, R., and Limarzi, J., “ITS at the Hudson Valley transportation management center,” IEEE Intell. Syst., vol. 19, no. 3, May-June 2004, pp. 8 - 12.

[22] Kelly, M., Folds, D., and Sobhi, N., “ATMS 2000: Hybrid automation or a lights out traffic management center?,” in Proc. Nat. Telesyst. Conf., June 16-17, 1993, pp. 37 - 42.

[23] Utamaphethai, N., and Ghosh, S., “Dicaf: a distributed architecture for intelligent transportation,” IEEE Computer, v. 31, no. 3, March 1998, pp. 78 - 84.

[24] Wu, J., Henson, L., and Amidon, J., “Distributed concept in ATMS software,” in Proc. IEEE Intell. Transp. Syst. Conf., Oct. 12-15, 2003, pp. 1295 - 1298.

[25] Huck, R., "A Study of the Requirements and the Design of the Intelligent Transportation System for the State of Oklahoma", Master's Thesis, University of Oklahoma, 2006.

[26] Brooke, K., Dopart, K., Smith, T., and Flannery, A., "Sharing Information between Public Safety and Transportation Agencies for Traffic Incident Management", Mitretek Systems, Inc., Washington, DC, 2004.

[27] Leibe, B., Schindler, K., Cornelis, N., and Van Gool, L., “Coupled object detection and tracking from static cameras and moving vehicles,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Accepted June 2008 for future publication.

[28] Baaziz, N., Lolo, N., Padilla, O, and Petngang, F., “Security and privacy protection for automated video surveillance,” 2007 IEEE International Symposium on Signal Processing and Information, December 2007, pp. 17 - 22.

[29] Green, M. W., “The appropriate and effective use of security technologies in U. S. schools,” U. S. Department of Justice, Report NJC178265, September 1999.

[30] Kilani, B., Vorakitolan, E., Havlicek, J., Tull, M., and Stevenson, A., “Distributed ITS Control and the Oklahoma Virtual TMC”, Proceedings of

the 12th International IEEE Conference on Intelligent Transportation Systems, St. Louis, MO,USA, October 3-7, 2009.

[31] Darter, M., Yen, K., Ravani, B., and Lasky, T., “Literature review of national developments in ATMS and opensource software,” California AHMCT Program, University of California at Davis and California Department of Transportation, Tech. Rep. F/CA/RI-2006/10, Dec 2006.

[32] Akkoumi, M., Huck, R., and Sluss, Jr., J., "A Personnel Detection Algorithm for an Intermodal Maritime Application of ITS Technology for Security at Port Facilities", submitted to the Journal of Transportation Technologies, July 2011.

[33] Dalal, N., and Triggs, B., “Histograms of oriented gradients for human detection”, IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Volume 1, June 2005, Pages: 886 – 893. (2005).

[34] Devarapalli, M., Sarangan, V. and Radhakrishnan, S., “AFSA: an efficient framework for fast RFID tag reading in dense environments”, Proceedings of the Fourth international Conference on Heterogeneous Networking For Quality, Reliability, Security and Robustness & Workshops, Vancouver, Canada, August 2007.

Appendices

Appendix A - Tulsa Port of Catoosa Demonstration Project Deliverable T.F.3

Appendix B - Assessment of Container and Cargo Integrity Sensor Alternatives Deliverable D.F.4

Appendix C - Aerial Surveillance Vehicles Augment Security at Shipping Ports

Appendix D - A Building Block Approach to Security at Shipping Ports

Appendix E - A Demonstration of a Low Cost Approach to Security at Shipping Facilities and Ports

Appendix F - Complete Bibliography for Robert Charles Huck