Hazardous Materials Safety and Security Technology Field Operational Test

Volume II:

Evaluation Final Report Synthesis

November 11, 2004

Contract No. DTFH61-96-C-00098; Task 9851

1. Report No. FHWA-OP-03-XXX	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Hazardous Materials Safety and Security Technology Field Operational Test Evaluation Final Report	**5. Report Date** November 11, 2004	
	6. Performing Organization Code	
7. Authors D. Stock (SAIC), M. Jensen (SAIC), M. Carter (SAIC), E. Wik (SAIC), C. Louisell (SAIC), and C. Mitchell (SAIC)	**8. Performing Organization Report No.**	
9. Performing Organization Name and Address Science Applications International Corporation (SAIC) 1710 SAIC Drive M/S T1-12-3 McLean, VA 22101	**10. Work Unit No. (TRAIS)**	
	11. Contract or Grant No. DTFH61-96-C-00098; Task 9851	
12. Sponsoring Agency Name and Address Federal Motor Carrier Safety Administration 400 7 th Street, S.W. Washington, D.C. 20590	**13. Type of Report and Period Covered**	
	14. Sponsoring Agency Code HOIT-1	

15. Supplementary Notes

Mr. Joseph DeLorenzo (FMCSA) (Task Manager)

Dr. Joseph I. Peters (COTR)

16. Abstract   This report provides the findings from SAIC's 2-year independent evaluation of the Hazardous Materials (HAZMAT) Safety and Security Technology Field Operational Test for the USDOT. This comprehensive report consists of the following three volumes:

Volume I: Executive Summary – This volume presents the overriding results generated from the evaluation of this FOT including overall benefit-cost results, industry deployment potential for FOT technologies, and policy options for consideration.

Volume II: Evaluation Final Report Synthesis – This volume provides information synthesized from the detailed reference sections contained in Volume III. This volume presents the "bottom line" results from the FOT activities.

Volume III: Evaluation Final Report Detail – This volume provides the five key reference documents used to support the evaluation and results for the HAZMAT FOT under one cover:

• Section 1: HAZMAT FOT Overview.

• Section 2: HAZMAT FOT Technical Performance, Efficiency and Safety Benefits Assessments.

• Section 3: HAZMAT FOT Security Benefits Assessment.

• Section 4: Benefit-Cost Assessment and Industry Deployment Potential.

• Section 5: Public Sector Component.

Key Words Hazardous Materials, Intelligent Transportation Systems, ITS Deployment; Security; National Test, Evaluation; Efficiency; ITS Technologies; Return on Investment; Risk Assessment; Motor Carrier; Trucking	**18. Distribution Statement** No restrictions. This document is available to the public from: The National Technical Information Service, Springfield, VA 22161.		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21.No of Pages** 123	**22. Price** N/A

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

FOREWORD

The following volume content definitions are provided to aid the reader in reviewing this detailed, multivolume effort presented as the Hazardous Materials (HAZMAT) Safety and Security Technology Field Operational Test (FOT) Evaluation Final Report.

Volume I: Executive Summary – This volume presents the overriding results generated from the evaluation of this FOT including overall benefit-cost results, industry deployment potential for FOT technologies, and policy options for consideration.

Volume II: Evaluation Final Report Synthesis – This volume provides information synthesized from the detailed reference sections contained in Volume III. This volume presents the "bottom line" results from the FOT activities, including the following topics, and concluding with potential policy options for consideration:

- The Importance of HAZMAT Security and the Need for Technology
- FOT Overview
- Evaluation Approach Overview
- Technical Performance
- Efficiency Assessment Findings
- Security Assessment Findings
- Safety Assessment Findings
- Benefits-Cost Results and Industry Deployment Potential
- Public Sector and Institutional Interfaces
- Potential Options to Realize Deployment Potential
- Conclusions

NOTE

> Volume III is a Sensitive Security Information document and is not available for public distribution.

Volume III: Evaluation Final Report Detail – This volume provides the five key reference documents used to support the evaluation and results for the HAZMAT FOT under one cover:

- **Section 1: HAZMAT FOT Overview.** This section provides the rationale behind this FOT, including a synopsis of FOT activities; identifies the FOT configuration; and describes the technologies deployed for this FOT.

- **Section 2: HAZMAT FOT Technical Performance, Efficiency and Safety Benefits Assessments.** This section outlines the baseline data collection effort and related technology prototype testing. This section presents quantitative and qualitative performance reviews of each of the individual deployed component technologies. The section includes the Efficiency and Safety Benefits Assessments that feeds into the Section 4 Benefit-Cost Assessment.

- **Section 3: HAZMAT FOT Security Benefits Assessment.** This section presents the Security Benefits Assessment and covers the analytical framework and Delphi process developed to support the Security Analysis and to feed the Benefit-Cost Assessment in Section 4.

- **Section 4: Benefit-Cost Assessment and Industry Deployment Potential.** This section presents the Efficiency, Safety and Security Benefit-Cost Assessments and Market Potential Analysis for Industry Deployment built upon the detailed Efficiency, Safety, and Security Benefits Assessments in Sections 2 and 3.

- **Section 5: Public Sector Component.** This section presents the evaluation of the Public Sector FOT, which is an add-on component to the larger HAZMAT FOT.

ACKNOWLEDGEMENTS

Expert Panelists:

ABBREVIATIONS

ANOVA	Analysis of Variance
ATA	American Trucking Association
ATRI	American Transportation Research Institute
BSG	Biometrics Solutions Group
BREW	Binary Runtime Environment for Wireless
CSI	Cambridge Systematics, Inc.
CMDA	Code Division Multiple Access
CPU	Central Processing Unit
CVSA	Commercial Vehicle Safety Alliance
CVO	Commercial Vehicle Operations
DHS	Department of Homeland Security
ESCM	Electronic Supply Chain Manifest
E-seal	Electronic Seal
FMCSA	Federal Motor Carrier Safety Administration
FMCSR	Federal Motor Carrier Safety Regulations
FOT	Field Operational Test
GPS	Global Positioning System
HAZMAT	Hazardous Materials
HMR	Hazardous Materials Regulations
IT	Information Technology
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
LTL	Less-than-Truckload
MCMIS	Motor Carrier Management Information System
MCSAP	Motor Carrier Safety Assistance Program
NAITC	North American International Trade Corridor
NMC	Network Management Center
NTTCA	National Tank Truck Carrier Association
OBC	On-Board Computer
P&D	Pickup and Delivery
PSRC	Public Sector Reporting Center
TSA	Transportation Security Administration
QTRACS®	QTRACS® is a registered trademark of QUALCOMM, for its fleet management messaging and vehicle tracking system.
ROI	Return on Investment
USDOT	U.S. Department of Transportation

1. HAZMAT SECURITY RISKS AND TECHNOLOGY SOLUTIONS

This synthesis document provides an overview of the Field Operational Test (FOT) and the processes, analytical frameworks and methods used to evaluate the Hazardous Materials (HAZMAT) Safety and Security Technology FOT. Also described are the approaches to assessing the operational efficiency and security benefits and costs, and findings and conclusions regarding potential benefits, costs, market potential, and deployment issues associated with the test technologies. Detailed information on the evaluation is contained within the reference **Volume III: Evaluation Final Report Detail, Sections 1 – 5**.

1.1   PROJECT CONTEXT

The HAZMAT movement chain presents an attractive target for terrorists due to multiple points of vulnerability that exist at manufacturing facilities, shippers, motor carriers, and shipment receivers. Hazardous materials are an especially sought after target since the nature of the cargo serves as a dangerous and ready-made weapon. Several hundred thousand HAZMAT shipments originate, travel en route, and are received every day, so the exposure to these vulnerabilities is very broad. Manufacturers and shippers may become terrorist targets due to potential HAZMAT production or storage at their facilities.

Motor carriers control the HAZMAT shipment en route between shipper and receiver. Since they transport 95 percent of hazardous materials, motor carriers are potentially targets for direct attack or hijacking for use as a weapon during en-route HAZMAT movements.

The immediate damage from a terrorist attack could be severe in terms of both human and economic losses. Human losses could include both injuries and death, with up to 10,000 casualties predicted under the most severe scenario considered in this study.

Economic losses could also be substantial. These losses would accrue most immediately to the affected shipper, motor carrier, receiver, and surrounding community. However, significant and perhaps even greater secondary economic impacts also may occur. These impacts may include disruption of the transportation industry; continuing business restrictions on HAZMAT manufacturers; potential damage to financial markets; and demoralization of the general public.

Myriad technology products are commercially available that are designed to enhance HAZMAT and transport security by making HAZMAT cargo more secure, less desirable to terrorists, and by reducing the consequences of intentional and non-intentional releases. Many of these technologies were tested and evaluated during the course of this HAZMAT FOT.

1.2   RESPONSE TO INCREASED NATIONAL SECURITY THREATS

The catastrophic events of September 11, 2001 and the ongoing war on terrorism have heightened the level of concern from Federal government officials and the transportation industry regarding the secure transport of hazardous materials. Security concerns focus on the potential of HAZMAT shipments as targets for terrorists. HAZMAT shipments through intermodal connectors, modes, and facilities are all attractive targets for terrorists, and pose a much greater concern to public safety than most other shipment types. HAZMAT shipments, especially fuels and chemicals, are especially attractive targets due to the multiple points of vulnerability. These vulnerabilities exist at shipper, motor carrier, and

shipment recipient facilities, and during shipment movement en route throughout the nation's roadway infrastructure.

Numerous international and domestic incidents occurred over the past several years that demonstrate the real threat potential that HAZMAT shipments pose. For example, the following events all occurred in a 2-month period in 2002:

- March 31, 2002: A 29-year-old driver for a propane distributor drove away with a 3,000-gallon bobtail. He made a telephone threat stating that he wanted to kill President George W. Bush and that he would use the bobtail as a "3,000-lb bomb".

- April 11, 2002: A terrorist driving a truck carrying liquefied natural gas ignited his cargo in front of a synagogue on the Tunisian Island of Djerba, killing 17 people, mainly German and French tourists. Al Qaeda claimed responsibility for the blast.

- May 16, 2002: A tractor-trailer carrying 10 tons of deadly cyanide in 96 drums was stolen after three armed men held up the vehicle north of Mexico City. Six drums were never found.

- May 2002: A fully loaded tanker truck pulled into Israel's largest fuel depot and suddenly caught fire due to an explosive charge connected to a cellular phone. The fire was extinguished, but had the truck exploded, destruction and death would have resulted.

Events such as these demonstrate the security and safety risks associated with HAZMAT shipments. The Federal Motor Carrier Safety Administration (FMCSA), working in close cooperation with the Transportation Security Administration (TSA), has attempted to proactively address public and private sector HAZMAT security concerns by identifying potential security risks related to HAZMAT transportation and proposing solutions to minimize those risks. FMCSA embarked on a program to improve HAZMAT security and safety by using regulatory measures, security assessments, and outreach efforts.

Part of this effort was to sponsor an industry competitive procurement. This led to FMCSA awarding a contract for a team led by the Battelle Memorial Institute (Battelle) (Deployment Team) to test currently existing major technologies that could offer solutions to minimize security risks of truck-based HAZMAT shipments. Supporting Deployment Team members included: QUALCOMM; the American Transportation Research Institute (ATRI); the Commercial Vehicle Safety Alliance (CVSA); SAVI Technologies; the Biometrics Solutions Group (BSG); and the Spill Center.

To evaluate the technologies tested in this FOT, their costs, benefits, and the operational processes require to be performed, the FMCSA, supported by the Intelligent Transportation Systems (ITS)-Joint Program Office (JPO), awarded an Independent Evaluation contract in August 2002. Science Applications International Corporation (SAIC) (Evaluation Team) led the Independent Evaluation for this HAZMAT FOT. The Evaluation Team also performed a key role in performing independent data collection and analysis activities for this effort.

1.3   PROJECT RATIONALE

The FMCSA is actively investigating methods to improve HAZMAT security. In parallel, the private sector has developed, or is currently developing a number of technological solutions that may offer security benefits. While several of these potential technological solutions have demonstrated efficiency benefits and some limited security benefits, most are not yet in widespread usage within the HAZMAT transportation industry. As such, the need existed for a national field operational test comprising complete suites of technology to address typical, specific HAZMAT operational scenarios.

The FMCSA sponsored this national FOT to demonstrate the effectiveness of technological system solutions to enhance safety and security. The FOT and accompanying evaluation may lead to the development of policies and incentives to promote deployment of the most promising technologies throughout the HAZMAT industry.

The purpose of this evaluation is to quantify all the relative costs of the deployed components and systems, and independently assess related security and efficiency benefits. While the functionality for various technologies was considered and tested during this FOT, it was not the Evaluation Team's intent to endorse any vendors for products tested during the evaluation process.

SAIC led the Evaluation Team effort with assistance from Cambridge Systematics, Inc. (CSI). The Evaluation Team coordinated activities with the Deployment Team to obtain quantitative and qualitative test-generated data and information. This data and information was used to independently develop the benefit-cost assessments for security and operational efficiency impacts on the HAZMAT delivery chain.

2. FOT OVERVIEW

2.1 PROJECT INTRODUCTION

In cooperation with industry, and on behalf of the FHWA, FMCSA sponsored the Hazardous Materials Safety and Security Technology Field Operational Test. The purpose of this project was to test methods for leveraging technology and operations to improve HAZMAT transport security and operational efficiency. The evaluation of this FOT quantified benefits resulting from technology deployments that improve the security and operational efficiency of HAZMAT shipments from origin to destination.

The Evaluation Team examined the degree to which the operational test fulfilled the stated objective of improving HAZMAT transport security and efficiency within discrete HAZMAT shipping scenarios. In addition, the Evaluation Team documented the HAZMAT shipments from origin to destination via a detailed benefit-cost assessment focusing separately on security and operational efficiency. The evaluation process ran parallel to project design and testing with consistent interaction with the Deployment Team to ensure timely bilateral project information exchange.

The FOT test duration was 18 months. The FOT testing period was 6 months for each of the nine motor carrier participants. The nine motor carrier participants had their deployment starts staggered to allow adequate time for proper technology installation, trouble shooting, data collection and technology de-installation. Specific timeframes for project activities are presented in Table 2-1.

Table 2-1. FOT Task Order Timeframe

Task Order	Timeframe
Task 1: Conducting Risk/Threat Assessment	September to December 2002
Task 2: Develop Concept of Operations	November 2003 to April 2004
Task 3: Develop System Requirements	January to April 2003
Task 4: Develop System Design	February to May 2003
Task 5: Conduct FOT	July 2003 to May 2004
Task 6: Evaluation	September 2002 to September 2004
Task 7: Deployment Team Final Report	June 2004
Task 8: Evaluation Team Final Report	September 2004

Within the parameters of the larger HAZMAT FOT, four states (New York, Texas, Illinois, and California) actively participated in the simultaneously conducted Public Sector add-on FOT, along with the accompanying law enforcement and emergency response agencies. These various agencies conducted staged scenario exercises to generate test data and provide enforcement officials' perspectives on security benefits for scenario-specific component and system technology applications. The Public Sector FOT and Evaluation are described in Section 8.

2.2   FOT TECHNOLOGIES

This section details the key functional and technical features for each of the component FOT technologies scheduled for deployment at the individual technology level. Technology descriptions not covered in this section are the various computer systems or servers that enable the core test component technologies to operate or integrate with one another. The following technologies are described:

- Wireless Satellite and Terrestrial Communications Systems

- Digital phone without GPS (not included in actual FOT deployment)

- Panic Buttons

- Global Login

- Biometric Global Login

- Electronic Supply Chain Manifest

- Intelligent On-Board Computers initiating remote vehicle disabling

- Internal Trailer Door Locking system

- External Electronic Seal

- Geofencing

- Tethered Trailer Tracking

- Untethered Trailer Tracking

It should be noted that this evaluation does not endorse any one vendor or another through the results of this evaluation or the functional product descriptions that follow. The evaluation's focus was to explore the functionality represented by the cited product types tested during the FOT. It was necessary for this test to consider individual products to collect quantitative and qualitative test data for the FOT. The specific products used in this FOT should be thought of as being representative for a class of products that exhibit similar functionalities in the field, and not as the only technology products to provide potential benefits in regard to HAZMAT security and operational efficiency.

Satellite/Wireless Terrestrial With GPS Communications Systems
Wireless Communications technologies were deployed for the FOT. This technology is designed to use Satellite-based global positioning system (GPS) technology to provide current vehicle positioning, including latitude and longitude readings. Another Wireless Communication system tested during the FOT was a Terrestrial-based communication link designed to allow two-way communications. Both Satellite and Terrestrial Communications are designed to generated vehicle position with every message. By design, position information for this FOT was generated upon request from the dispatch computer, and position-reporting frequency was configurable at the system user's discretion. Mobile-initiated position-reporting rate is normally configured at 1-hour intervals.

Some FOT participant carriers utilized macros that provide preformatted "fill-in-the-blank" messages, which are more cost-effective than free-form messages, can be updated over the air, and are easily defined by fleet management. All messages are also acknowledged and have a return receipt option.

Digital Phone Without GPS

This technology permits transmission of integrated work order assignment and status messaging between motor carrier dispatch and driver utilizing a Binary Runtime Environment for Wireless (BREW)-enabled digital cellular handset unit. Table 2-1 displays two code division multiple access (CDMA) BREW phones.

Figure 2-1. CDMA BREW Phones.

Software applications allow a carrier the capability to send a driver a load assignment that the driver will accept or reject. Upon load acceptance, the driver is provided with specific details pertaining to the particular load assignment. The software applications enable drivers to send and receive up to five macros pertaining to progress conditions for each load assignment:

- Accept/Reject Load assignment

- Arrived

- Started

- Stopped

- Departed

Panic Buttons

"Panic Button" technology enabled a driver to remotely send an emergency alert notification message either via Satellite or Terrestrial Communications, and/or utilize the remote Panic Button to disable the vehicle. The Panic Button was deployed in two physical configurations, which are displayed in Figure 2-2:

- A Panic Button mounted inside the vehicle to send an emergency alert notification.

- A wireless Panic Button that can be carried by the driver to remotely send an emergency alert and/or use the remote Panic Button to disable the vehicle. The wireless Panic Button is carried by the driver and has a range of 150 feet.
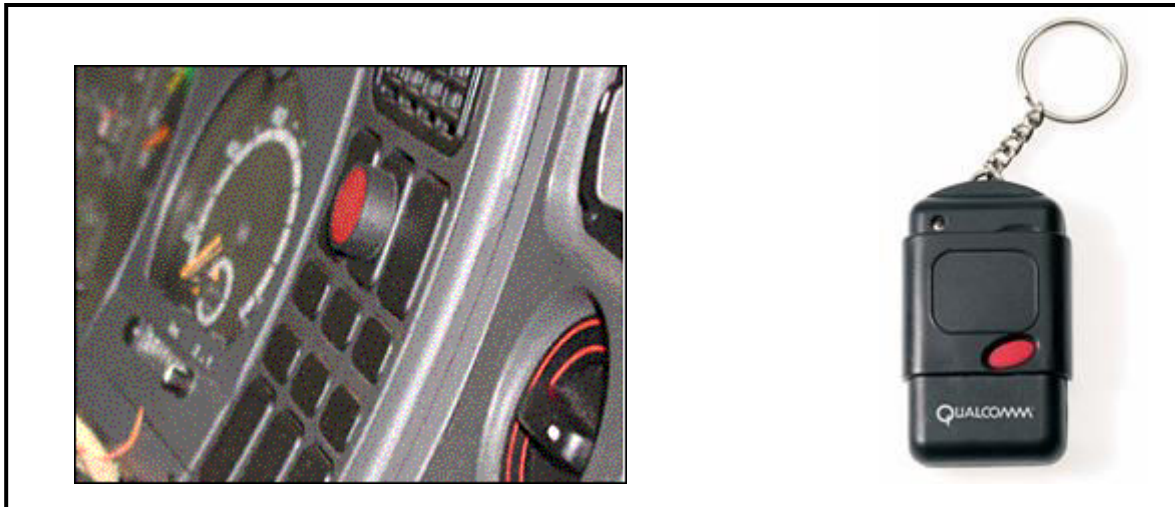
Figure 2-2. Dash-Mounted Panic Button and Wireless Panic Button.

Global Login

Global Login is an identification technology, which is enabled via the Wireless Communication system maintained by on-board software. A driver entered login information (consisting of a user identifier [ID] and password) into a cab-based interface. The login information was verified within the truck and remotely using the Wireless Communication system. If the Global Login failed, alert notifications were sent to the motor carrier for further action, including vehicle disabling.

Biometric Global Login

Biometric Global Login was accomplished via a biometric verification unit in the motor vehicle as displayed in Figure 2-3. The Biometric system consists of a Central Processing Unit (CPU) and proprietary firmware that managed a smart card reader and fingerprint scanner to execute biometric verification on the driver. By design, the biometric system for this operational test operated with the on-board communications systems.

Figure 2-3. Biometric Fingerprint Reader.

Electronic Supply Chain Manifest

The electronic supply chain manifest (ESCM) system was designed to provide positive personnel (chain of custody) identification and load tracking capabilities for the parties involved with cargo shipments. The ESCM system integrated biometric verification, smart cards, Internet applications, and on-board Wireless Communications.

During the FOT, the ESCM system was initiated with a shipper biometrically logging onto the system and creating an electronic manifest, as well as identifying the load assignment. Upon completion of the electronic manifest, the shipper transmitted the manifest to a secure central server and logged out. All authorized users were notified via e-mail regarding the manifest submission. The HAZMAT shipment information was then stored and routed through a central database. All authorized users were required to log-on biometrically to gain access to the ESCM at any point in the shipment. Also, encrypted "smart cards" containing vital shipper, cargo, and driver information were used to transfer and validate HAZMAT shipment movement information. Figure 2-4 shows the ESCM visible to FOT participants displaying manifesting information and manifest transfer details.[1]

Figure 2-4. ESCM Screen with Manifest Details and Transfer Information.

Intelligent On-Board Computers

The On-Board Computer (OBC) was integrated with the Wireless Communications/vehicle operating systems. The OBC permitted the motor vehicle to be disabled in the event of a security breach. These disabling techniques included blocking fuel or sending instructions via the Wireless Communications system directly to the vehicle's data bus, which caused loss of throttle power to the motor vehicle. The OBC also was configured to shut down the vehicle whenever there was a loss of satellite signal strength, such as when cables are tampered with or the receiver unit is covered. One variant of the vehicle disabling capability that did not require the use of the OBC was *local vehicle disabling*. By the driver depressing the panic button of his key fob, a signal was sent directly to the vehicle to initiate the disablement. The wireless panic button with local disabling capability is carried by the driver and has a range of up to 250 feet. This latter application does not require the OBC to perform the local vehicle disablement.

Internal Trailer Door Lock

The internal door locks enabled a dispatcher with the ability to lock and unlock trailer door locks via an over-the-air command. Upon arrival at the consignee's location, the driver sent

---

[1]Battelle, *HAZMAT Safety and Security Field Operational Test Task 4: System Requirements and Design*, May 1, 2003.

trailer "door unlock" requests to the dispatcher. The dispatcher then sent an unlock command upon verification of the driver request. Requests to lock and unlock the doors were sent to the dispatcher using the Wireless Communication System. The OBC then facilitates the execution of the lock and unlock events. A specific button installed in the dash of the truck signals the driver as to when the trailer doors can be securely opened.

Once the unlock command has been sent and the driver has pressed the "door open" button, the driver normally had 20 seconds to open the doors before the doors would automatically relock. If the doors relock before the driver is able to open them, the driver contacted the dispatcher to request that the dispatcher resend the door open command.

Figure 2-5 displays the Internal Door Lock installed in the rear door of a motor vehicle trailer in this FOT.

Figure 2-5. Internal Cargo Door Lock.

External Electronic Seal

The wireless electronic tag seal (E-seal) system used for this FOT is a Web-based application designed to automatically generate an alert notification when a seal is compromised without proper authorization. The E-seal used short-range Wireless Communications to interface with a mobile E-seal reader in the vehicle. The mobile reader was connected to the on-board Wireless Communications device and the cargo alert notifications were transmitted automatically to the dispatcher. Figure 2-6 displays the E-seal in its distinctive rugged black box.

Figure 2-6. Electronic Seal.

<u>**Geofencing**</u>
Internet-based Geofencing and route-monitoring capabilities are designed to allow authorized users to define a risk area or route to monitor. An "electronic fence" can be placed around the route or designated landmark on a displayable Internet-based map. If a driver deviates from a specified route or approaches a risk area, the Geofencing system should notify the dispatcher. If the vehicle enters the risk area, an alert notification should be sent to the carrier's dispatch center. Figure 2-7 (on the next page) displays one of screens that a dispatcher may view when tracking a Geofenced motor vehicle.

<u>**Tethered Trailer Tracking**</u>
For this FOT, Tethered Trailer Tracking was designed to allow dispatchers to remotely monitor trailer "connect" and "disconnect" events. Tethered Trailer Tracking should allow users to view connect and disconnect events are by the installed mobile unit and transmitted to dispatch across a satellite link with information on the date, time, and connect/disconnect location.

<u>**Untethered Trailer Tracking**</u>
For this FOT, a proof of concept of this product was used to test Untethered Trailer Tracking capabilities. This tracking system used the core wireless satellite tracking system, including Geofencing capabilities. Merging a tethered and an untethered device documented functionality for an untethered design.

The Untethered Trailer Tracking system is designed to provide real-time trailer identification regarding connect/disconnect time and location, Geofencing, and unscheduled movement. The system used a multimode Terrestrial Wireless Communications technology designed to provide more geographic coverage by eliminating blackouts and "dead" zones.
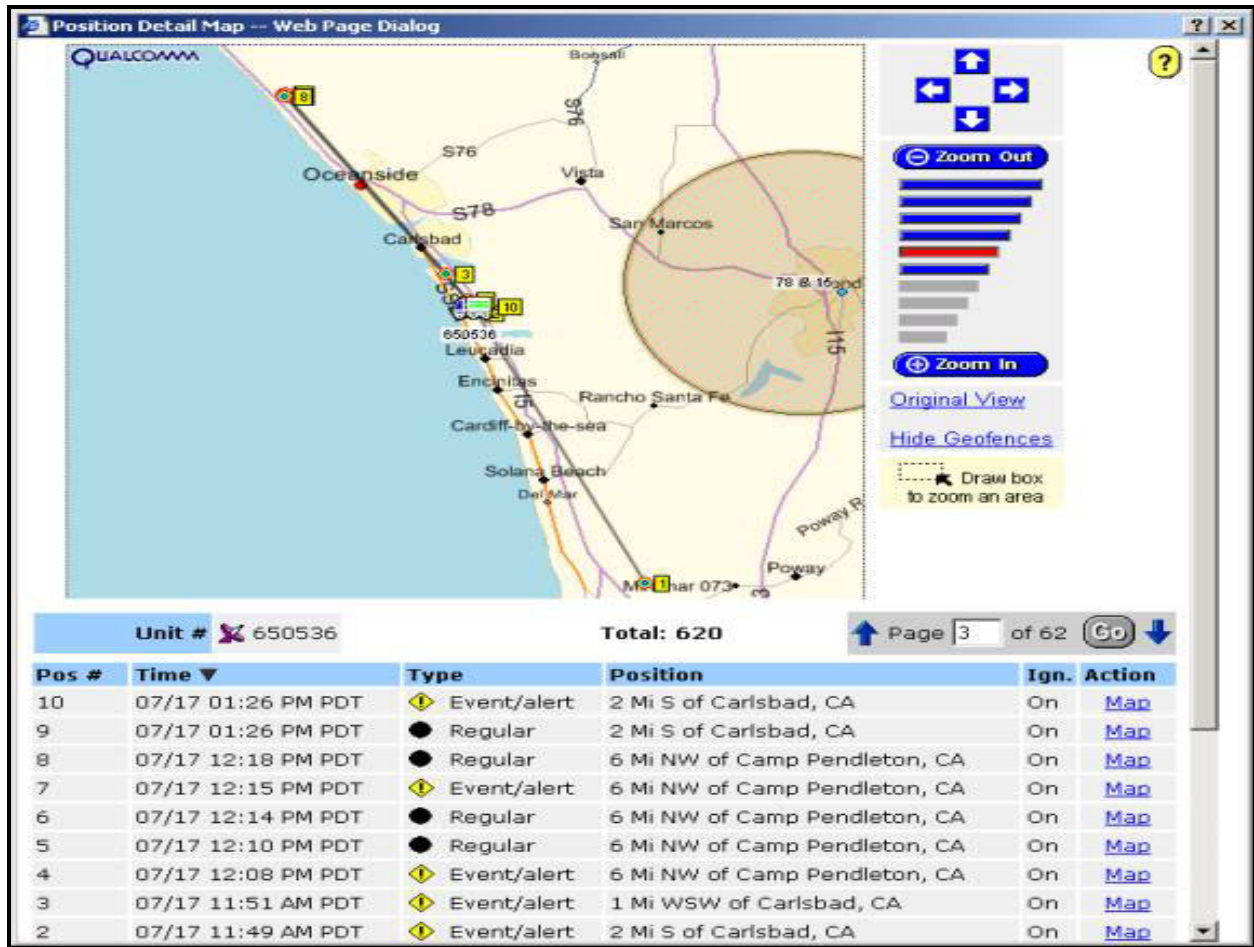
Figure 2-7. Geofencing Dispatch Display Map.

2.3 SYSTEM ARCHICTECTURE

The system architecture was designed by the Deployment Team to meet the specified requirements of the FMCSA Operation Test. Figure 2-8 depicts the System Architecture for the FMCSA Operational Test.[2] Specific technical system details can be found in **Volume III**, **Section 2: HAZMAT FOT Technical Performance, Efficiency and Safety Benefits Assessments**.

---

[2]Battelle, *HAZMAT Safety and Security Field Operational Test: Task 4 System Requirements and Design*. May 1, 2003.
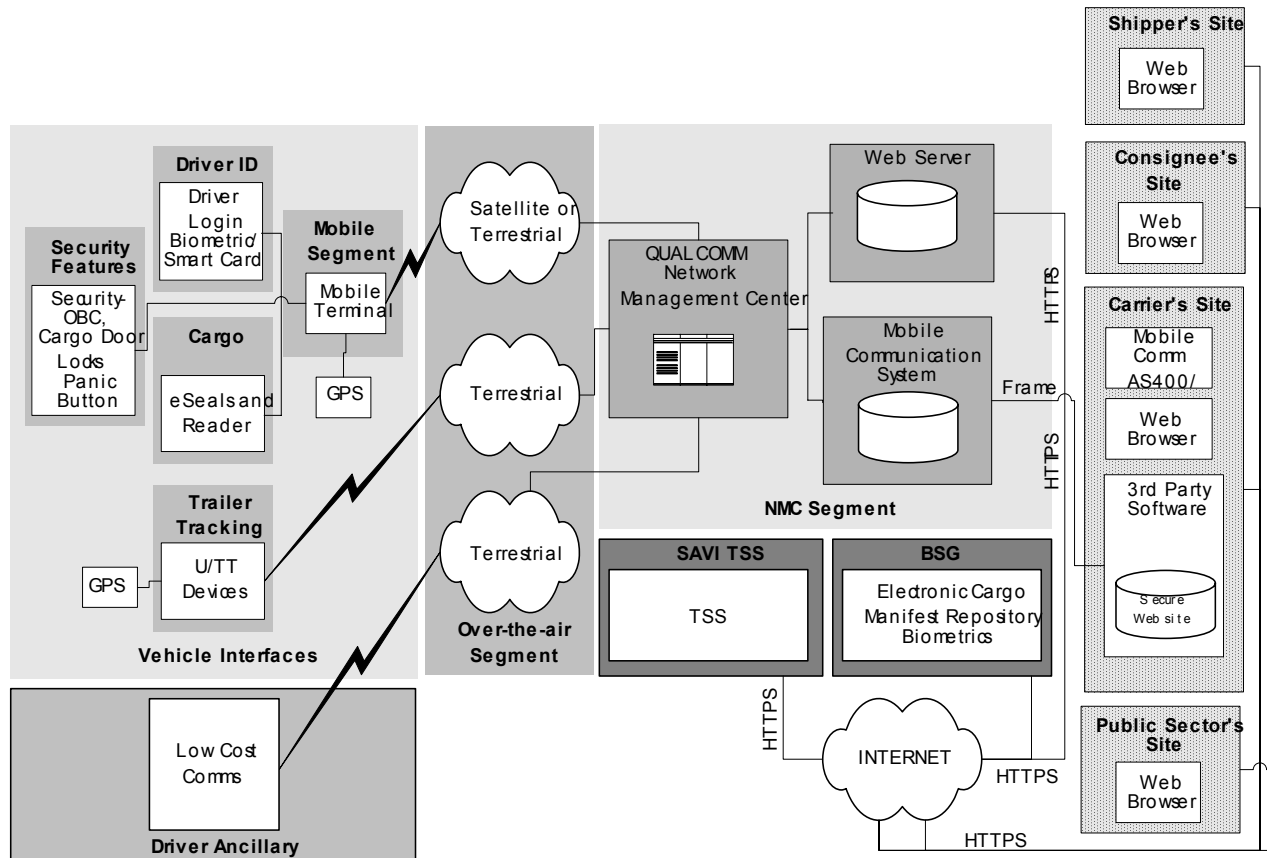
Figure 2-8. HAZMAT Safety and Security FOT System Architecture.

2.4   FOT SCENARIOS

The FOT was separated into four operational scenarios to allow each scenario to address a distinct segment of the HAZMAT transportation market. Each scenario deployed a unique set of technology solutions to account for the specific operational characteristics for a particular sector of the HAZMAT market. The selected technological solutions for each scenario sought to improve security and operational efficiency at several cost levels, depending on the comprehensiveness of the deployed technology set. The four general scenarios for this FOT included:

- Scenario 1: Bulk Fuel Delivery

- Scenario 2: Less Than Truckload High Hazard

- Scenario 3: Bulk Chemical

- Scenario 4: Truckload Explosives

Table 2-2 provides a complete overview display of the multiple scenarios for this test including motor carrier participants, shippers, consignees, Public Sector state agency participants, routes, test technologies, and HAZMAT cargo classifications for each of the FOT designed scenarios. More specifics about each motor carrier participant are provided in **Volume III, Section 1: HAZMAT FOT Overview.**

The four scenarios were all scrutinized against security risk profiles that categorize and prioritize risk based on the potential tactics terrorists might use, the most likely hazardous materials that could be involved, and by the of the type of shipment – bulk/truckload or less-than-truckload (LTL). The rationale for this risk analysis was to determine potential security gaps that might exist for each scenario.

Table 2-2. Overall FOT Scenario Composition

Scenario	# Trucks	Shipper	Carrier	Con-signee	State Agency	Routes	Tech-nologies	HAZMAT Cargo
1a	13	Exxon Mobile	Dupre Transport	Exxon Mobile	TxDPS	Texas – 120 mile radius of Dallas, San Antonio, Austin	Satellite Comm., Panic Dash, Global Login	Bulk Fuel Delivery – Class 3 Flammable Liquid
1b	12	Exxon Mobile	Cox Petroleum	Exxon Mobile	CHP	California – from Vernon, CA to central and southern CA	Satellite Comm., Panic Dash, WPB	Bulk Fuel Delivery – Class 3 Flammable Liquid
2a	12	GE Betz & Hercules	Distribution Technologies	• UT/Battelle • Progressive Energy • SC Electric & Gas • Westinghouse Nuclear • Eglin AFB	N/A	Macon or Reynolds GA to TN, NC, SC, Fl	Satellite Comm., Panic Dash, Global Login, OBC	LTL–High Hazard • Hydrochloric Acid (Class 8 Corrosive) • Polyester Resin (Class 3 Flammable) • Perchorylethelene (Class 6.1 Poison)
2b	13	Various	Roadway Express	Various	N/A	Various	Terrestrial Comm.	LTL–High Hazard • Pick up & Delivery
3a	12	Dow Chemical	Transport Services	NuFarm Americas, Inc.	ISP	Midland, MI to Chicago Heights, IL	Satellite Comm., Panic Dash, WPB, Bio. Auth., ESCM	Bulk • Acetronitrile (Class 3 Flammable) • Aqua Ammonia (Class 2.2 Non Flammable) • Nitric Acid (# 8 Corrosive)
3b	7	BP Chemical	Quality Distribution	• Eli Lily • Pharmacia • Lonza	N/A	Lima OH to IN, MI, PA	Satellite Comm., Panic Dash, WPB, Bio. Auth., ESCM	Bulk • Acetronitrile (Class 3 Flammable)
3c	6	BP Chemical	Roeder Cartage	Evans Chemical	NYSP & NYDOT	Lima OH to Waterloo, NY	Satellite Comm., Panic Dash, WPB, Bio. Auth., ESCM	Bulk • Acetronitrile (Class 3 Flammable)
4a	12	Orica USA	R&R Trucking	Orica USA	NYSP & NYDOT	Charlestown IN to NY, NJ, & IL Joplin, MO to TX	Satellite Comm., Panic Dash, WPB, Bio. Auth., ESCM, OBC, Electronic Seals, Geofencing	Truckload Explosives (Class 1.1-1.6)
4b	13	Dyno Nobel	Dyno Transportation	Dyno Nobel	ISP & CHP	Joplin, MO to Pittsfield, IL and Lincoln, CA	Satellite Comm., Panic Dash, WPB, Bio. Auth., ESCM, Untethered / Tethered Trailer Tracking	Truckload Explosives (Class 1.1-1.6)

3. EVALUATION APPROACH

3.1   EVALUATION OVERVIEW

The primary intent of the FOT was to determine the extent to which existing vulnerabilities in the transportation of hazardous materials can be reduced, thereby reducing the potential for a catastrophic event with resulting loss of life and property. The benefit-cost analysis was designed to measure this benefit and determine which component technologies or integrated systems offer the best mix of improved security balanced against reasonable costs for deployment and operations.

Deploying these technologies and systems will require an investment by the trucking industry, which is an industry with very low returns – a profit margin of 2 percent is not uncommon. An important aspect of this evaluation was to determine whether or not the deployment of these technologies and systems would generate a positive return on investment for industry. The potential return from deployment was quantified as a measurable improvement in operating efficiencies or improvement in overall operations. The objective assessment of this "bottom line" impact is critical for determining policy options for structuring a deployment program: market-based, where operating efficiencies drive deployment; or a mandate in the interests of national security; or a package of incentives designed to encourage and facilitate deployment.

3.2   ASSESSMENT FRAMEWORKS

The main evaluation impact categories examined by the Evaluation Team are safety, security, and operational efficiency. As detailed in Figure 3-1, these impact categories feed the benefit-cost analysis according to macroeconomic/societal (macro) public sector benefit-cost results (stemming from security and safety benefits) and microeconomic/industry (micro) private sector benefit-cost results (derived from operational efficiency improvements and enhanced safety). The macro/societal and micro/industry benefit-cost measurements analysis was conducted to determine the following:

- Are the industry operational efficiency benefits significant enough to drive widespread industry deployment of test technology systems?

- If not, are the macro benefits large enough to warrant government action to facilitate wide-scale national deployment?

The evaluation assessments were conducted within the scope of the FOT and extended the FOT findings to the larger universe of truck-based HAZMAT shipments (for the four primary load types) through rigorous analytical frameworks. These frameworks utilized primary and secondary industry survey data; detailed motor carrier census records; market analysis of technology products and services that are commercially available; and the opinions provided by two august groups of leading national experts in HAZMAT shipping, public safety, security and risk assessment – an Expert Steering Committee and a 26-member Delphi Panel.

The assessments determined what measurable benefits exist, and established and implemented analytical frameworks to monetize potential benefits and to weigh these against any costs that would have to be incurred to realize the benefits. Detailed discussion of methodology are presented in **Volume III, Section 3: HAZMAT FOT Security Benefits Assessment** and **Section 4: Benefit-Cost Analysis and Industry Deployment Potential**, and are summarized in the following sections of this synthesis document.
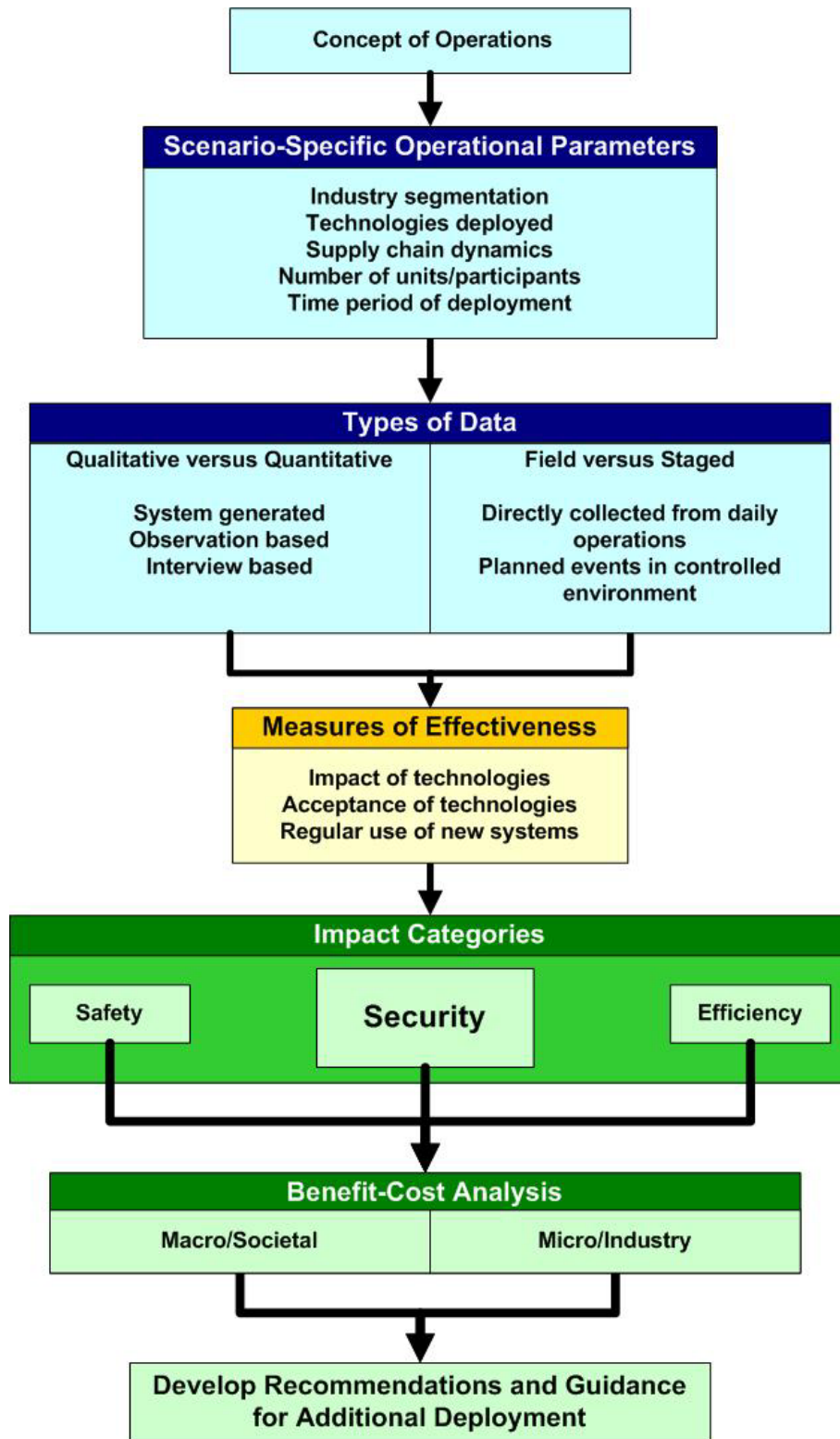
Figure 3-1. Evaluation Framework.

It should be noted that the test technologies were designed to enable real-time communications and information exchange among drivers, dispatchers and other authorized parties; to track assets; to secure vehicles, loads, and shipping documentation; and to enable driver or automated exception alerts in response to crises or deviations in operational characteristics outside of set parameters. The technologies themselves and their usage are not specifically designed to provide explicit or traditional safety benefits (i.e., reducing the frequency and severity of crashes).

The test technologies are not designed to warn drivers of obstacles in proximity to their vehicles, lane departure, imminent vehicle rollover conditions, or conditions signaling driver fatigue. The exceptions include the beneficial impacts of frequent driver/dispatcher communications that allow a dispatcher to assess the driver's condition; position tracking to determine possible speeding, or capabilities that provide responders to HAZMAT incidents timely notification of the incident; and location and the type and quantity of HAZMAT involved to enhance the rapidity and appropriateness of response. Potential safety benefits in terms of crashes avoided and enhanced emergency response are proffered, but are mostly qualitative in nature. Quantitatively, the evaluation focused on the remaining two key assessment areas: Security and Operational Efficiency.

The estimation of benefits and costs, payback periods, and industry deployment potential was based on a stepwise analytical framework. Benefits were derived as operational improvements and reductions in potential impacts of terrorist activities involving truck-based HAZMAT shipments. The framework for these assessments (as illustrated in Figures 3-2 and 3-3) is based on the following inputs:

- Technology performance and participant perceptions, as defined by the FOT, established technology functionality, efficacy, user acceptance, and operational improvements. These data also provided inputs to the Delphi process described in **Volume III, Section 3**.

- HAZMAT carrier demographics (total number of trucks and fleet size distributions) for each load type that was included in the FOT. These data, defined through queries of the FMCSA's Motor Carrier Management Information System (MCMIS), established the number of trucks that would represent potential full deployment of the test technologies. The results of the Deployment Team's motor carrier survey. Returned by 153 motor carriers, the respondent demographics represented a broad diversity of fleet sizes, range of operations, routing variability, general operational characteristics and levels of fleet management technologies currently used and those to be employed in the near-term. These results were validated using other industry technology deployment studies and applied to the demographics of HAZMAT carriers reported in the FMCSA Motor Carrier Management Information System (MCMIS) database to estimate levels of current technology market penetration and total market potential.[3]

- A Technology Compendium, which defined current and near-future levels of motor carrier technology adoption, and pricing and functionality of commercially available technology products with similar capabilities as the technologies testing during the FOT. The latter provided a range of potential industry costs.

Other important evaluation goals included: assessing technical performance of the test suites; user acceptance and perceptions of the pros and cons of using the technologies;

---

[3] ATA Foundation, *Motor Carrier Technologies – Fleet Operational Impacts and Implications for Intelligent Transportation Systems/Commercial Vehicle Operations*, October 1999; ATA Foundation, *NAFTA Priority Corridor Comprehensive ITS/CVO Plan Motor Carrier Technology Survey,* August 2000; American Transportation Research Institute – GartnerG2, *Trucking Technology Survey*, 2003.

issues of deployment costs; privacy and the potential for governmental intervention; and defining the market potential for the deployment of the technologies.

The data were collected through direct observations; reviews of technology transaction records; interviews and survey questionnaires of motor carrier and state agency participants and non-participants; and consultation of secondary data sources. These assessments are the basis for the overall evaluation findings.

The processes involved in the Efficiency and Security Assessments are detailed in **Volume III, Sections 2 and 3**, respectively, and are summarized in the sections that follow.
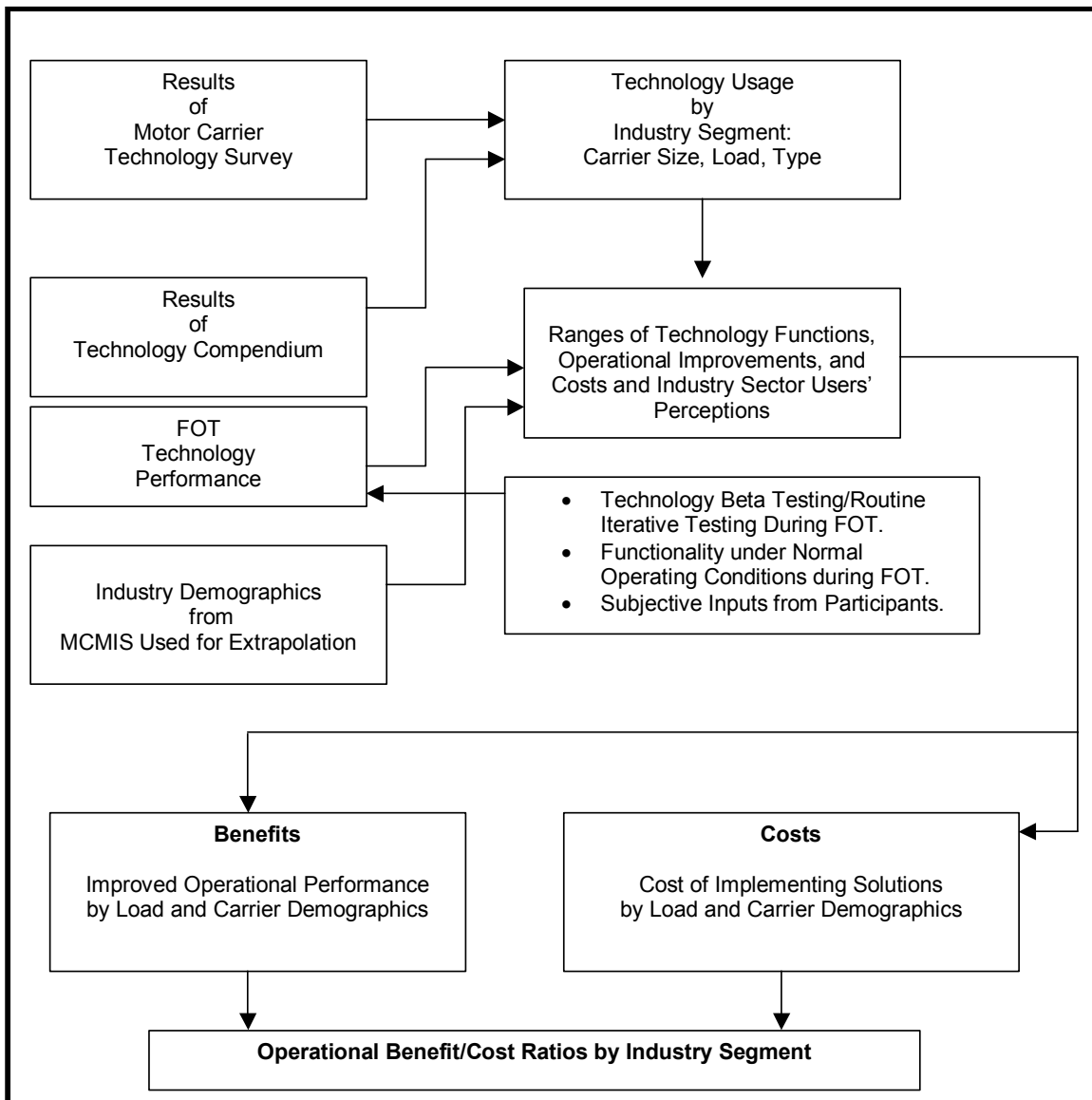
Figure 3-2. Operational Efficiency Benefit-Cost Analysis Process Flows.
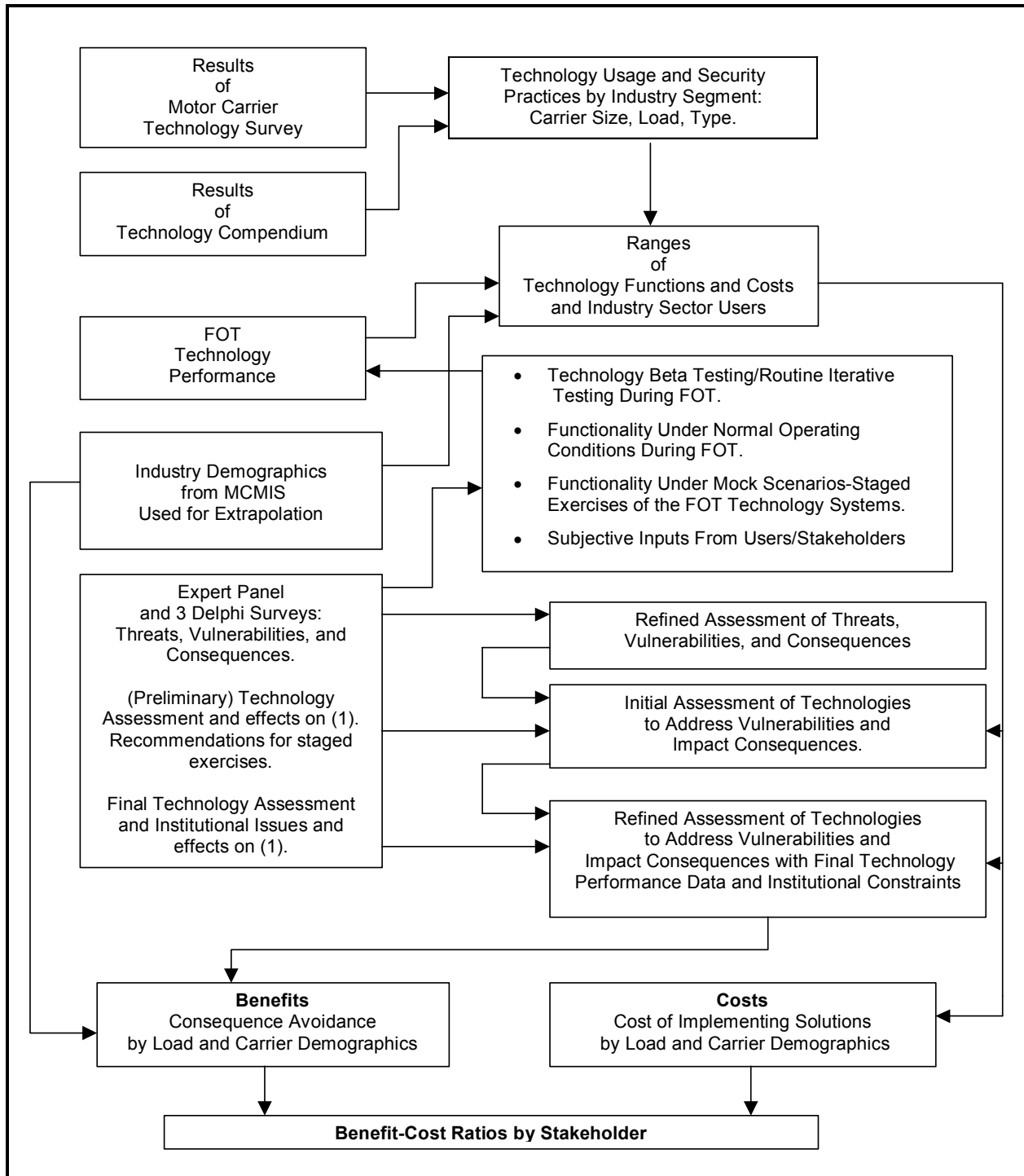
Figure 3-3. Security Benefit-Cost Analysis Process Flows.

4. TECHNICAL FOT PERFORMANCE

Technical performance of the FOT technologies was demonstrated through initial Beta Testing, then during the operational test through technology exercises and staged security events. In these latter tests, the systems were tested in the field under near real-world conditions. Additionally, day-to-day performance of the test technologies' performance was captured via participant interviews and analysis of archived event transaction logs.

4.1   TECHNOLOGY FOT PERFORMANCE

The following subsections summarize the motor carrier participants' reactions to the test technologies, as well as transaction volumes collected for the FOT by technology over the 6-month test periods for the motor carrier FOT participants. The Deployment Team archived comprehensive data records and forwarded this information on a monthly basis to the Evaluation Team for independent analysis.

4.2   BASELINE PARTICIPANT INTERVIEWS

On-site baseline interviews were conducted with FOT participant carriers to confirm the "day in the life" descriptions provided in the Concept of Operations document prepared by Battelle.[4] These interviews were also used to collect all available operations data to be used in comparison with the FOT automated system-generated operations data. These on-site interviews aided in quantifying existing operations, including key operating metrics, and provided the availability to collect qualitative perspectives. These perceptions were collected from the terminal managers, dispatch operations staff, and drivers. Collecting baseline data from this series of on-site visits enabled a thorough analysis, leading to informed judgment regarding the effectiveness of test component and test system technology to improve HAZMAT security and operational efficiency.

These on-site FOT participant interviews initiated the process of establishing quantitative and qualitative baseline data for each of the eight FOT participant sites interviewed. Eight of the FOT participant carriers were interviewed at either their operations terminal or corporate headquarters during the summer of 2003. The ninth FOT participant, the Scenario 1A participant motor carrier, was interviewed by phone. Follow-up occurred by regularly scheduled site visits during the FOT to obtain necessary quantitative and qualitative information required to effectively evaluate test technology and test systems' impacts on security and operational efficiency. Some of the general topic areas examined in the on-site FOT participant interviews included:

- Baseline operational description/processes, or "day-in-the-life" descriptions.
- Leading security issues and concerns.
- Current operational and security procedures with or without test technologies.
- Pre-test participant expectations of technology and test outcomes.
- An inventory of technologies and in what combinations the fleets currently employ, including decision support and record-keeping back office systems.
- Current performance measures used in fleets.

---

[4] Battelle, *HAZMAT Safety and Security Field Operational Test: Task 2: Concept of Operations*, prepared for FMCSA, April 18, 2003.

- Data used to support performance measurement and decision-making – data types, formats, frequencies, collection, and processing lags (current or historical).

- Currently used carrier return on investment (ROI) models/analyses. Where the participants conducted such analyses and were willing to share these results with the Evaluation Team, the analyses were used to provide historic baseline data and provide a framework for overlaying FOT-generated data for a side-by-side comparison of impacts.

- Historical (archived) data streams – either internal or vendor processed. These included paper logs or electronic records of dispatch; pickup and delivery events and times; and miles traveled en route.

4.3   OVERALL BASELINE SITE VISIT RESULTS

The reactions from FOT participant carriers interviewed have been overwhelmingly positive. All participants worked well with the Evaluation Team to provide comprehensive short-term historical data for comparison with system-generated test data. Interviewees expressed enthusiasm for the FOT, and many stated an extreme interest in the test outcome, especially if any government mandates result from the FOT findings. It should be noted that the first two site visits were in a slightly different format than the latter six visits that more formally followed the interview guide developed by the Evaluation Team.

4.4   TECHNOLOGY EXERCISES

The Evaluation Team also collected independent data via interim on-site visits with selected FOT participants in December 2003. This effort was conducted to verify and collect functional data/information concerning test technologies at FOT participant sites in an operational setting. These on-site visits also enabled the Evaluation Team to collect qualitative FOT participant user reactions up to the midpoint of this FOT. These interim interviews captured a broad range of user attitudes, perceptions, reactions, and policy options generated from several months of exposure and use of deployed test technologies at the respective FOT sites.

During the December technology exercises, FOT technologies were tested numerous times in varying configurations to validate their functional integrity for field operations. These technology exercises enabled the Evaluation Team to collect additional technology performance data for FOT participants to bolster the data sample used for analysis.

The technology exercises tested the "real-world" efficacy of the technologies and examined the technical and procedural success or failures. These exercises yielded policy options for improvements in technical performance, content and presentation of exception alerts, or operational procedures to maximize the use of the FOT technology-generated information.

Technologies targeted for exercising during the site visits were those that would not necessarily be used in daily trucking operations (i.e., Panic Buttons, Vehicle Disablement). Additionally, the Evaluation Team wanted to observe ESCM use, system login procedures, and to instigate, if possible, failure of the login process.

Following are the summary technology testing results for technology exercises conducted during December 2003:

- **Dash Panic Button with Notification:** 47 seconds average time to send and receive panic alert (9 test events).

- **Wireless Panic Button with Notification:** 44 seconds average time to send and receive panic alert (12 test events).

- **Wireless Panic Button with Local Disabling:** Tested successfully all 10 times it was tried. Disabling occurred on test vehicles immediately after the panic button initiated throttle release.

- **Global Login:** 33 seconds average for driver verification using Global Login (15 test events).

- **Global Login:** 38 seconds average for unsuccessful login for Global Login (12 test events)

- **Biometric Global Login:** 55 seconds average for driver verification using Biometric Global Login (12 test events).

- **Biometric Global Login:** 11 successful test events detecting the fingerprint tested did not match the fingerprint on the smart card.

- **OBC with Remote Disabling:** 2 successful test events with dispatcher initiating throttle disable at driver request with an average time of 20 seconds.

4.5   STAGED EVENTS

Staged test events were designed to assess the efficacy of the FOT test suites in terms of technical and procedural performance to address key threats and vulnerabilities. In addition to technical testing of the FOT technologies, similar to the technology exercise testing, these events were designed to exercise the full integration of the technology suites. The FOT also tested the technology/human interface to effectively detect and respond to staged attacks on HAZMAT shipments.

The Evaluation Team conducted staged event testing from mid-February to mid-April 2004 at five FOT participant carriers covering all four operational test scenarios. These events allowed for selected FOT technologies to be tested in the most simple and complicated system technology configurations.

There were seven distinct staged event types, with each corresponding to a specific threat type or identified vulnerability, as defined here:

- **Geofence Violations:** Vehicle violates Geofence in normal course of operations.

- **Driver Panic Alerts:** While vehicle is en route, the driver triggers a panic alert.

- **Driver Identification:** In the course of a truck trip, driver fails login – staged at pickup or delivery point or as part of enforcement inspection process.

- **Untethered Trailer Tracking:** Vehicle violation of trailer Geofence ("unauthorized" movement of trailer).

- **Electronic Seal Breaches:** Electronic seal tampering en route.

- **Load Tracking (ESCM):** Sending erroneous manifests – location of delivery, units, load type to public and private sector test participants.

- **Vehicle Disabling:** Disable vehicle via driver local disabling, dispatch/enforcement disabling, or OBC with loss of signal disabling via OBC in a controlled environment.

Each test event type was repeated several times per involved carrier. Staged event participants were notified of scheduled test events before the testing took place. Test event data was gathered via on-site observation and debriefing interviews immediately after staged events. Additionally, the Evaluation Team analyzed system time-stamped event data and collated it to other collected data.

The staged events helped to identify the aspects of response procedures that are not as well supported by the technologies as they could be, including identifying potential system improvements. Relevant information and data from the technology exercises was also presented to the Delphi Panelists to enable them to provide informed opinions regarding the technologies' ability to reduce vulnerabilities.

4.6   FOT TECHNOLOGY USE AND PARTICIPANT TECHNOLOGY REACTIONS

FOT participants' reactions to the various technologies deployed during the course of testing were documented at several points during the FOT. Most notable were the opinions collected during the final exit interviews at the conclusion of the FOT during April and May 2004. Exit interviews were conducted onsite at seven FOT participants; the other two were conducted via conference call.

The opinions expressed at the midpoint and conclusion of the FOT concerning various issues related to the technologies under test did not change significantly. Overall, perceptions were positive for the motor carrier FOT participants, with the most notable exception being the Biometric Login. This technology resulted in usability problems for both drivers and employees trying to access the ESCM system via the Biometric Login.

Table 4-1captures general participant response to overall technology configurations at the mid point and completion of the FOT. The scale used in capturing the participants' opinions ran from 1 equaling "Strongly Disagree" to 5 equaling "Strongly Agree."

Table 4-1. Participant Responses to General Technology Reactions

Participant Reaction Statements	Interim Findings 1=Strongly Disagree; 5=Strongly Agree	Final Findings 1=Strongly Disagree; 5=Strongly Agree
1. The deployed test technologies made a favorable impression upon yourself and others at your company?	3.7	4
2. The test technologies have been used significantly and on a regular basis?	3.7	4
3. The test technologies have not required significant staff resources including time?	3	4
4. The initial training provided adequate to prepare personnel to use the test technologies?	4	3
5. The drivers have responded positively to using the test technologies?	3.5	3.6
6. The test technologies system might prove to be an improvement to your existing operations?	4	3.9
7. The test technologies have been easy to use?	4	4.
8. The test technologies have been reliable?	4.2	3.9
9. The test technologies have allowed for better/easier tracking of loads, drivers, and vehicles?	4.3	4.7
10. The test technologies have improved customer service and Estimated Time of Arrivals for pick-ups and deliveries?	4.3	4.6
11. The test technologies have provided an increased sense security and safety for company employees?	3.4	3.5
12. The test technologies have been effective at providing the following functionalities during the test period to date. - Securing a Shipment - Incident Response - Driver Identification - Route Deviation - Load Tracking	4.7 4.3 4 4 4	4 4.3 4.2 4 4.3

The following information presents the test technology transaction volumes and qualitative FOT participant opinions for each of the deployed test technologies. The Evaluation Team collected this information throughout the FOT via archived FOT transaction logs, direct observation, on-site FOT interviews, surveys, and phone interviews.

Wireless Satellite Communications/Wireless Terrestrial Communications

- Wireless Satellite Communications Vehicle Position Reports: 572,804 events

- Forward Messages/Macros from Dispatch to Vehicle: 57,074 events

- Return Messages/Macros from Vehicle to Dispatch: 256,191 events

Eight of the nine FOT test participants have been using Wireless Satellite/Terrestrial Communications for significant periods of time prior to this FOT. Participants unanimously praised Wireless Satellite/Terrestrial Communications. All eight participant carriers that have previously and continued to use Wireless Satellite Communications affirmed the positive efficiency impact it has had on their operations, and all showed robust technology utilization for Wireless Satellite Communications. Positioning frequency ranged from 17 to 70 minutes for FOT participants that depended operational conditions, such as desired customer reporting frequency, type of commodity being hauled, and length of route. Table 4-2 displays the transaction volumes for the Vehicle Position Reports and mean time between position reports received from Wireless Satellite/Terrestrial Communications by specific scenario.

**Table 4-2. Vehicle Position Reports from Wireless Satellite/
Terrestrial Communications by Motor Carrier**

Vehicle Position Reports		
Scenario	**Transaction Volumes**	**Mean Time Between Position Reports**[5]
Scenario IA	120,840	32 min 53 sec
Scenario 1B	159,031	29 min 02 sec
Scenario 2A	33,280	59 min 18 sec
Scenario 2B	91,727	17 min 30 sec
Scenario 3A	38,898	63 min 39 sec
Scenario 3B	32,418	58 min 22 sec
Scenario 3C	16,128	70 min 24 sec
Scenario 4A	47,384	48 min 58 sec
Scenario 4B	33,098	59 min 14 sec
TOTAL TRANSACTIONS	**572,804**	

FOT participants agree on the positive efficiency benefits derived from using Wireless Satellite/Terrestrial Communications. These communications methods allow motor carriers to better manage drivers and vehicles. Wireless technology enables a dispatcher to rapidly locate company trucks at any time and from any location. Dispatchers utilized the Wireless Satellite tracking to respond to customer location inquiries for their loads. Carriers enjoyed the ability to run detailed reports off archived position records. Companies consistently mentioned that drivers tend to more efficient in managing their time when Wireless Satellite Communications were installed in their fleets. This helps improve carrier productivity and enhance customer service on the return on investment (ROI) side.

Some participants also heavily used macro messages going between dispatcher and driver and vice-versa during this FOT. Using macros allows operational information to be quickly relayed either to or from a terminal and a remote fleet. Table 4-3 displays the transaction volumes for the Forward Messages/Macros from dispatch to vehicle by specific scenario.

---

[5] Intervals less than 3 minutes and over 12 hours have been eliminated from the data set because at the low end, the interval represents part of message traffic between driver and dispatcher related to a single "conversation"; above 12 hours represents vehicles that are parked long term and do not generate position reports.

Table 4-3. Forward Messages/Macros from Dispatch to Vehicle Transactions by Motor Carrier

Forward Messages/Macros from Dispatch to Vehicle	
Scenario	Transaction Volumes
Scenario 1A	29,526
Scenario 1B	14,987
Scenario 2B	9,739
Scenario 3A	2,693
Scenario 3B	1
Scenario 3C	128
TOTAL TRANSACTIONS	57,074

Table 4-4 displays the transaction volumes for the Return Messages/Macros from vehicle to dispatch by specific scenario.

Table 4-4. Return Messages/Macros from Vehicle to Dispatch Transactions by Motor Carrier

Return Messages/Macros from Vehicle to Dispatch	
Scenario	Transaction Volumes
Scenario 1A	56,884
Scenario 1B	98,240
Scenario 2A	5,616
Scenario 2B	71,390
Scenario 3A	9,490
Scenario 3B	6,715
Scenario 3C	489
Scenario 4A	5,796
Scenario 4B	1,571
TOTAL TRANSACTIONS	256,191

On the security side, Wireless Communications increased the perception of driver, vehicle, and cargo security through near constant visibility. Motor carriers report knowing about stolen vehicles being recovered quickly when Wireless Satellite Systems were in use for a fleet, although none of these events occurred during the conduct of the FOT. Drivers initially resisted the idea of being monitored, but have grown accustomed to the concept, and now, many report feeling more secure knowing that their locations are known.

Digital Phone Without GPS

The Digital Phone without GPS was not tested during the FOT deployment. The participant who was scheduled to use the phones for the FOT could not accommodate the phones into the company's daily operational processes after initially assessing the technology's feasibility. Prior to deploying in operational testing, management assessed the feasibility of sending load tender messages to driver phones, and then had a driver use the phone to perform selected macros. The limited test macros worked well according to the carrier, and the technology was considered viable, but would need to be improved in several areas for trucking companies to commercially use this application. Specific comments for improvement included:

- The phone's display is small, and may be difficult to see for some of our older drivers. Also, the menu button is very difficult, even with practice, to navigate the menus and selections.

- The cellular coverage in the carrier's test area was not good once the drivers left the interstate highway.

- Battery life on the phones was short, which required the phone to be plugged into the cigarette charge adapter most of the time.

- The phones are not equipped with a GPS capability. This would be a useful feature for carriers who need to know where the driver is located to validate the information.

Global Login

- Global Login/Biometric Login: 78,891 events

Global Login is an enhanced driver login system that provides password verification for participating drivers. Global Login is only available on satellite mobile units. The Global Login process uses a database at the Network Management Center (NMC) that has a record for each driver. Each satellite mobile unit maintains a small driver list, which holds information for up to five drivers. When the mobile unit is first initialized, there are no drivers in the list. As new drivers log in, they are added to the driver list.

Each driver record includes the following information:

- Driver ID or user name

- Password

- Full Name

For the FOT, there were six distinct event record types captured by the QUALCOMM archived data and delivered monthly to the Evaluation Team for Global Login:

- Global Driver Log In

- Global Driver Log Off

- Bad Log In

- Driver Bumped Off

- Distance Exceeded without correct Log In.

- Time Exceeded without correct Log In.

Several test participants for driver identification and verification in the commercial motor vehicle cab used Global Login heavily during this test. Global Login proved useful for ensuring driver identity by simply entering a username and code into the mobile

communications unit. Global Login proved to be a reliable form of driver identification at the four carriers who were assigned Global Login for this FOT. Several other carriers used Global Login as a backup to Biometric Login when it failed.

Global Login was generally well received by drivers who found that training was brief and simple, especially when compared to the Biometric Login. Drivers found that Global Login did not impede their daily operations.

The time required for Global Login was relatively consistent across FOT participants. The Evaluation observed at least five Global Login events at three FOT participant carriers. Global Login events were completed successfully several times at each site in about 33 seconds. Incorrect Global Login events were also conducted to show the ability of the system to reliably detect incorrect login attempts under operational conditions. Incorrect Global Logins also take approximately 38 seconds for the system to detect.

The following summarizes the timings observed at the participant motor carriers:

Successful Global Login by carrier:

- Transport Services (33.4-second average – 5 test events)

- Cox Petroleum (32.6-second average – 5 test events)

- Distribution Technologies (34-second average – 5 test events)

Unsuccessful Global Login by carrier:

- Transport Services (42-second average – 2 test events)

- Cox Petroleum (37.8-second average – 5 test events)

- Distribution Technologies (37-second average – 5 test events)

One petroleum carrier noted that the Global Login provided good security for driver identity. Another petroleum carrier thought that the Global Login might be a burden to some of its drivers who make many stops, but management admitted that the technology worked well. Both of the petroleum carriers noted that perhaps Biometrics would be a more convenient method of identifying drivers than the Global Login application deployed in this FOT.

Biometric Login

- Global Login/Biometric Login: 78,891 events

The Biometric system consisted of a Central Processing Unit (CPU) with proprietary firmware that controls an attached smart card reader and fingerprint scanner that performed Biometric verification. The Biometric system was customized to communicate with the on-board communications systems. The on-board Biometrics device is integrated using Global Login.

For the FOT, there were six distinct event record types captured by the QUALCOMM archived data and delivered monthly to the Evaluation Team for Biometric Global Login:

- Global Driver Log In

- Global Driver Log Off

- Bad Log In

- Driver Bumped Off

- Distance Exceeded without correct Log In

- Time Exceeded without correct Log In

The Biometric Login caused the most frustration of any technology deployed in this FOT due to design and functionality issues. This is disheartening, because the concept of the Biometric Login appealed to many of the participant carriers as a potential means to improve driver identification or employee identification to gain access to cargo load information.

The actual experience that test participants had with the Biometric Login device used in this FOT was that it was often unreliable in the field due to the difficulty in finger placement. It is necessary for users to introduce consistent fingerprints into the Biometric reader to allow either the vehicle to properly start or for employees to log into the ESCM system to work with manifest files. Driver complaints were high for this technology in regards to usability in the field.

According to the FOT participants, for the Biometric fingerprint Readers to be useful in a motor carrier environment, the Readers need some overall design improvement. In addition to difficulty in finger placement location for participants, other problems were noted as well. For example, if a driver's finger were too hot or too cold, the Biometric Reader would often fail to obtain a successful login event. Drivers became frustrated with the device over time and would either stop using it altogether or use the Global Login feature as a backup.

Biometric Login was relatively reliable under test exercising conducted at participant sites during the FOT. The Evaluation Team observed at least five logins per site at three FOT participant carriers using both correct Biometric Login procedures and using procedures to create a login failure (i.e., incorrect code entry, wrong fingerprint, and cold hands).

The purpose of this exercise was to observe the processes; reiterate the findings of the automated data; and to obtain driver opinions about the process and their experience in using the systems. Biometric Logins ranged from about 45 seconds to 1 minute to successfully compete or to detect an unsuccessful attempt.

Global Login and Biometric Login Data

Global Login and Biometric Login data is presented here together since data archives display the same data for both types and several carriers used both types of logins during this FOT.

The numbers below show the totals for successful and unsuccessful global and biometric logins during the course of this FOT:

- Successful Global/Biometric Login: 20,092 events.

- Unsuccessful Global/Biometric Login: 864 events.

Table 4-5 displays the login total for the Global Login/Biometric Login by the specific scenario. Table 4-6 (on page 31) displays the Global Login event types by percent recorded during the FOT.

Table 4-5. Global Login/Biometric Login Transactions by Motor Carrier

Global Login/Biometric Login	
Scenario	**Login Totals**
Scenario 1A	30,579
Scenario 1B	27,470
Scenario 2A	2,960
Scenario 3A	1,119
Scenario 3B	1,997
Scenario 3C	4,438
Scenario 4A	3,607
Scenario 4B	6,721
TOTAL TRANSACTIONS	**78,891**

Electronic Supply Chain Manifest

- The ESCM system generated 55 identifiable, unique manifest numbers. The following numbers describe various manifest transactions that occurred using the ESCM system:

- 4 manifests list only one event, such as "create", with no release or other activity.

- 20 manifests were created and released with no further activity.

- 19 manifests were created, released, picked up, and transferred, but not delivered to a shipper or trucking company.

- 12 manifests represented complete shipments from shipper to trucking company to consignee.

The event records for ESCM were captured and archived in the Biometric Solutions Group (BSG) server and forwarded to the Evaluation Team monthly. The types of events captured in these records included:

- Transaction time and date

- User name

- Shipper name

- Carrier name

- Consignee name

- Transaction Type (create, transfer, pick up, release or delivery)

The electronic supply chain manifest (ESCM) system process is initiated with a shipper biometrically logging onto the system and creating an electronic manifest, identifying the load assignment. After the appropriate data fields are completed (the system notifies the user if essential fields are incomplete or incorrectly filled out), the shipper initiates data transmission and information to a secure central server and logs out. All identified partners are notified via e-mail of the submission.

Although the FOT participants considered the ESCM to be a good concept, participants felt that all stakeholders needed to be involved in the transaction to make it successful.

Table 4-6. Global Login/Biometric Login Event Type Percentage Usage by Scenario

Event	Scenario 1A	Scenario 1B	Scenario 2A	Scenario 3A	Scenario 3B	Scenario 3C	Scenario 4A	Scenario 4B
GL Bad Login	0.1%	0.1%	0.3%	18.5%	6.4%	21.4%	7.0%	4.8%
GL Distance Exceeded	9.8%	9.8%	5.3%	1.2%	5.0%	2.7%	11.0%	7.3%
GL Driver Bumped Off	1.4%	2.8%	0.0%	0.1%	0.0%	0.0%	0.0%	0.1%
GL Driver Login	29.9%	28.4%	35.9%	40.0%	36.5%	26.8%	31.3%	32.0%
GL Driver Logoff	28.5%	25.6%	33.4%	36.8%	34.2%	24.3%	30.1%	30.5%
GL Time Exceeded	30.3%	33.3%	25.1%	3.3%	17.8%	24.8%	20.6%	25.1%

Note: Scenario 2B participant did not use Global Login for this FOT.

Shippers, carriers, consignees must all participate. ESCM is not useful as a stand-alone system. All stakeholders need to be plugged into the same interface to make this sort of technology application useful and beneficial.

Access to shipment status was a major benefit noted by participant carriers who noted that it would be useful for both internal and external consumption. The ESCM was useful for viewing manifest information prior to customer pickup for the motor carriers. The manifest information provided precise commodity and quantity data for the dispatcher to see and relay that information to the driver in the field. Customer inquiries on shipment status could be quickly responded to by accessing the ESCM Website.

Participants expressed that the ESCM could reduce paperwork errors and reduce the amount of times needed to enter shipment information across the supply chain. The ESCM was viewed as a system that could also help reduce the accounts receivable cycle by a several days by allowing simultaneous invoice creation with delivery confirmation. An additional assessment was that ESCM would be useful if it was integrated with the carriers' dispatch system, rather than being a stand-alone system. ESCM was viewed as a tool that could help law enforcement or emergency response personnel know the contents of a truck to decide how to properly respond to an incident.

Overall, ESCM usage was poor during the course of the FOT. Although five carriers used the ESCM technology, none used it on a consistent basis. Some of this poor usage can be blamed on the problems encountered with the Biometric Login. Other problems were noted as well. In some instances, either shippers or consignees did not participate much or at all in the ESCM process. This would cause carrier usage to drop as well as isolating the carriers from their business partners in trying out a new technology. The repetitive nature of having to use the ESCM along with traditional paper based processes for a test shipment consumed time and effort for test participant staffs.

During the course of the FOT, the Evaluation Team observed differences in use between the ESCM processes and those with clerical methods and manual paperwork processes. Processing times for manifests were usually in the 2- to 3-minute range for non-ESCM events, versus about 1minute for ESCM events.

The ESCM system seems to be a technology that demands a high level of attention from the Operational Team to ensure consistent system usage over a prolonged period of time, such as what was required for this FOT. The ESCM needs to be used more frequently and consistently in future testing environments to generate more data on which to substantiate efficiency benefits that stakeholders suggest are potentially there.

Panic Buttons

- Panic Button Message Events: 118 test events (not actual panic alerts from drivers)

Panic Buttons were tested under controlled conditions during this FOT such as on-site technology exercises and staged events testing. Table 4-7 displays the number of Panic Button Message events recorded by the specific motor carrier, though these were not actual panic alerts generated by the drivers. There were no accidental panic alerts generated during this FOT. All panic alerts were "created" during on site testing, technology exercises or staged events testing.

Table 4-7. Panic Button Message Events by Motor Carrier

Panic Button Message Events	
Motor Carrier	**Number of Events**
Scenario 1A	9
Scenario 1B	25
Scenario 2A	17
Scenario 3A	24
Scenario 3B	6
Scenario 3C	18
Scenario 4A	6
Scenario 4B	13
TOTAL TRANSACTIONS	**118**

This technology was well accepted by the motor carriers. It was felt that Panic Buttons could accurately provide the location and time of an alert event when pressed by a driver in distress. Panic Buttons were viewed as having excellent security potential. In fact, several of the participants already had in-dash Panic Buttons installed prior to this FOT and expressed excellent satisfaction with the technology. Panic Buttons are mandatory for motor carriers participating in the Defense Transportation Tracking System and are required for Department of Transportation and Department of Energy for transporting certain load types, such as munitions.

Panic Buttons were generally well received by drivers and dispatchers, and provided a sense of security to many of the drivers. Panic Buttons were viewed as a viable technology method to alert the motor carrier or law enforcement personnel from remote regions of the nation. The only issue associated with the Panic Button was that some drivers felt the key fob (security token) design could cause an alert to be issued by a driver by accidentally bumping the trigger device.

Panic Buttons were also combined with the remote disabling available to the driver when in the immediate vicinity of the truck for some of the FOT participants. Participants viewed this as a way for a driver to respond directly to disable the vehicle in the event that an unauthorized party attempted to gain vehicle control. Drivers seemed to enthusiastic about this technology application that put the ability to disable a vehicle into their own hands.

During site visits at five FOT participant carriers, participants were asked to activate the Panic Button with notification configurations from two to three times per vehicle. Panic Buttons were not tested during normal operations due to the sensitive nature of the technology and not creating "false alarms". Recorded panic alert notifications from the technology exercise site visits took between 25 seconds to about 1 minute from the moment the Panic Button was pressed to the point when the dispatcher was alerted at the motor carrier facility.

Wireless Panic Button with Local Disabling was demonstrated of capability a minimum of two times per participant site for five participant carriers. The vehicle was disabled at distances

up to 250 feet from the vehicle location. During these tests, successful throttle disablement occurred almost immediately when a Panic Button was pressed at the test locations.

Geofencing

- Geofence Events: 165 Off Route Detections
  79 On Route Detections
  38 Geofence Violations
  38 Exited Geofence Area

Geofencing was utilized in two operational functionalities during this FOT by one of the FOT participants. Geofencing is used for alerting a trucking company when one of its vehicles leaves its designated route or enters a restricted area. Both functionalities involved frequent vehicle positioning via Wireless Satellite Communications.

The first of these functionalities, off-route detection, was tested from mid-January to mid-April by one of the FOT participant carriers on selected routes. Typically, one truck, but sometimes more, was selected daily during this 3-month test run to have a .5-mile zone placed on both sides of a delivery route designated for a vehicle. Each time a vehicle position report is generated, the vehicle position is compared against the specific route created on the QTRACS®[6] Web interface. The default positioning is set for once an hour, and is configurable at the discretion of each carrier.

Each time a positioning event takes place, this technology compares the position report against a software-created map to determine that a vehicle is not "off route" or inside or outside a designated "Geofence". This time is set at the default 1-hour positioning frequency, but the actual comparison rate depends on a particular carrier's message frequency. The participant positioning intervals observed in the FOT varied due to hourly position reports, message traffic-which provides position, and vehicle downtime en route. These included:

- Scenario IA: 32 min 53 sec

- Scenario 1B: 29 min 02 sec

- Scenario 2A: 59 min 18 sec

- Scenario 2B: 17 min 30 sec

- Scenario 3A: 63 min 39 sec

- Scenario 3B: 58 min 22 sec

- Scenario 3C: 70 min 24 sec

- Scenario 4A: 48 min 58 sec

- Scenario 4B: 59 min 14 sec

The carrier participant in this FOT had a positioning frequency average of 48 minutes and 58 seconds due to hourly position reporting and message traffic.

Once an off-route violation was detected, the alert message was sent out within 30 seconds to 1 minute to the dispatcher's screen. Off-route detection can be set to increase the polling rate for vehicle positioning once an off-route event is detected – a feature that was not utilized during the FOT by the testing participant. There was no evidence in the archived

---

[6] QTRACS® is a registered trademark of QUALCOMM for its fleet management messaging and vehicle tracking system.

records or through contact with the dispatcher that at any point the off route detection failed to work properly.

There were 165 off-route detection events during this FOT and 79 on-route detection events, signifying that a vehicle had returned to its designated route. There were more off-route detections because a vehicle might take a different route to the delivery location than the dispatcher-selected route. Drivers were not told what vehicles on what days were being used for off-route detection.

Minimal training was needed for the dispatcher to set a route. Each time a route was selected, the dispatcher entered the route by mapping points on an Internet-based software package. It was reported that the dispatcher would like to have the ability to archive historical routes for future usage. This would eliminate the need for the dispatcher to create a route from scratch by designating selected points on the virtual map.

The second functionality, Geofencing to alert of trucks entering a "keep out" or restricted area, was tested from late February to late April at two selected sites. The first of these sites was the participant terminal; the second site was the O'Fallon Inspection Station near O'Fallon, Illinois. A 2-mile radius was placed around each location. In the case of the latter test, the violated geofence breech occurred between two position reports generated 29 minutes apart.

Participating test trucks caused Geofence detection either when the truck violated the geofence by entering the 2-mile radius surrounding the restricted area or when the truck exited the restricted area. Each time a vehicle position report is generated, the vehicle position is compared against the specific "keep out" or "keep in" radius created on the QTRACS® Web interface. The default positioning is set for once an hour, and is configurable at the discretion of each carrier.

In the same manner as off-route detection, it took up to 1 hour to for the system to detect an "off route" or Geofence violation based on the standard 1 hour positioning frequency. Once this Geofence violation was detected, the alert message was sent out within 30 seconds to 1 minute to the dispatcher's screen. There was no evidence in the archived records or through contact with the dispatcher that at any point the geofence detection failed to work properly. Geofence detection can be set up to increase the polling rate for vehicle positioning once a Geofence event is detected – a feature not utilized during the FOT by the testing participant.

Geofencing was received positively by the FOT participant who used it during the FOT. The participant viewed Geofencing as an excellent technology to locate a vehicle that was off route or in an area where management did not want that truck to be positioned. The participant thought it would useful as a tool not only to improve security, but it might keep drivers from stopping for excessive periods of time at unauthorized locations. Geofencing did not change driver behavior directly since the drivers were not aware of what vehicles were being monitored with Geofencing.

There were limitations to Geofencing in the manner that it was utilized in this test. With positioning frequency default set at 1 hour, it is possible for a vehicle to enter a "Geofence" or to travel "off route" and not be detected as long as at the location of the next positioning event the vehicle is back on course or no longer in the "Geofence" zone.

The simplest answer is to increase vehicle-positioning frequency, but more frequent positioning than 1-hour intervals would become costly for many motor carriers. Geofencing technology needs to cost effectively develop the functionality to detect violations and report them in more near real time. The technology should ideally trigger a violation alert in real time rather than needing to wait for the next positioning report to activate the alert.

Electronic Seals

- Electronic Seal Events: Security Events 3,553 and Inspection Inquiries 1,151

By definition, *security events* were comprised of the necessary steps to remotely operate the electronic seal including assigning, locking, unlocking, and unassigning the seal. These events are all covered in the specific archived functionalities listed below with the exception of "Inspect Asset Security". By definition, *inspection inquiries* were the user requests for remote asset status updates that may be made at any point in the HAZMAT distribution chain and were recorded as an "Inspect Asset Security".

The following electronic seal events were archived during this FOT:

- Assign Seal
- Lock Seal
- Validate Security
- Un Assign Seal
- Inspect Asset Security
- Synchronize Seal
- Unlock Seal
- Clear Tamper Status

The wireless electronic tag seal (E-seal) system used for this test is a Web-based application that provides continuous online security monitoring of cargo containers and other assets. With the wireless electronic tag seal system, the user should be able to verify that a container was loaded and sealed at a secure loading point and sealing station. The E-seal can provide information regarding tamper events to ensure container accountability from point of origin to destination. For this application, the mobile Wireless Communications system was used as the communications link between its site-based and mobile subsystems.

The E-seals were also created as a concept of technology utilizing existing hardware, but not specifically for a truck environment. The participant saw potential value to the E-seal as a security device, but operational problems with the electronic seal tested including low reliability and heavy driver time and involvement needed to operate the electronic seals.

E-seals were difficult for drivers to operate at the onset of the test. It took between 5 to 6 minutes to complete the cycle of assigning and locking an E-seal at a customer's pick-up location. This problem was remedied when these steps were combined into a single step to reduce the time to between 2 and 3 minutes. Training was also difficult for the drivers, due to the complexity of the technology, and the many steps involved in its operation.

During the "staged events" testing in April 2004, initial attempts to communicate with E-seals attached to the trailer's rear door were unsuccessful, while E-seals placed on the sides of the trailer were detected. This is position in which the E-seal would normally be placed in real-

world operations. Upon closer examination, the E-seal engineers discovered that the trailer selected for this test was constructed of extremely heavy gauge, double-walled stainless steel. The mechanic who selected the trailer used in the test stated that it was a newer model, and that it was the heaviest-duty trailer in the company's fleet. The E-seals had to be moved away from the heavy doors and onto the sides of the trailer; only then did the Reader in the vehicle cab read all three seals.

The electronic seal as tested in this FOT does not demonstrate a realistic operational device at this point.

OBC With Remote Door Lock

- Remote Trailer Door Lock: 16 events

This technology was successfully utilized 16 times with no recorded unsuccessful technology events by the participant carrier who had the OBC with Remote Door Lock installed on one truck for FOT testing. The participant observed that the OBC with Remote Door Locking had some merit as a security device at an acceptable cost for the carrier. The driver must send a message via the OBC unit to the dispatcher for permission to unlock the door. The dispatcher must then send an over-the-air command to remotely unlock the trailer door. The driver had 60 seconds to unlock the door after receiving confirmation from the dispatcher; otherwise, the driver would have to call again to gain permission to open the door. The amount of time the driver was allowed before the door opens is configurable according to user requirements.

The OBC with Door Lock worked excellent in both daily operations and during on-site technology testing. This sequence of events was demonstrated during on-site testing at the FOT participant carrier using this functionality on one truck. Due to the door/lock construction, it is difficult for an unauthorized individual to pry the doors open. Even if an unauthorized party opened the doors, a tamper message would be sent to the Network Management Center (NMC) that the doors security has been breached. The motor carrier or law enforcement can then be contacted about the situation.

OBC With Remote Disabling/Loss of Signal Disabling
This technology was well received during on site technology testing and during "staged events" testing at several of the FOT participants. Participants did seem to have reservations about shutting down vehicles in the normal stream of traffic, but viewed it as an option in emergency situations. Participants thought it difficult to imagine this technology being deployed in the real world due to these concerns.

Tethered/Untethered Trailer Tracking

- Trailer Tracking: Tethered Trailer 362 Events (connects and disconnects) and Untethered Position 7,133 Reports

Tethered Trailer Tracking allowed dispatch to monitor trailer connects and disconnects. Connects and disconnects were detected by the mobile unit and passed on to dispatch via the satellite link with the date, time, and location. Tethered Trailer Tracking required that each trailer be equipped with a transmitter that communicated to the mobile unit on the vehicle DC power bus. Archived FOT data included the trailer ID, the event code to either connect or disconnect, and the system time of the event.

Untethered Trailer Tracking allowed for real-time trailer identification, connect/disconnect time location, Geofencing, and unscheduled movement of the trailer independent of any power requirements or connectivity with the vehicle cab. The system utilized a multi-mode terrestrial wireless technology, which provided better geographic coverage by eliminating blackouts and dead spots, thereby improving reliability and service over single mode systems.

Both the Tethered and Untethered Trailer Tracking technologies were well received by the FOT participant using these technologies. Dispatch found useful the ability to detect trailer connects and disconnects with the Tethered Trailer Tracking, and the ability to track an unconnected trailer as another authorized carrier moved it. Both technologies were used on a consistent basis during the FOT.

5. EFFICIENCY BENEFITS ASSESSMENT

The goal of this Efficiency Assessment is to define and estimate the test technologies suites' ability to enhance motor carriers' financial performance and determine whether efficiency gains, if any, are adequate to induce motor carrier investment.

5.1   APPROACH TO DETERMINING TECHNOLOGY EFFICIENCY BENEFITS

As described in *Evaluation Technical Memorandum 4: Motor Carrier FOT ROI and Performance Measures*,[7] the calculation of operational benefits, associated with the FOT technologies is one component of the broader benefit-cost assessment, detailed in **Volume III, Section 2**, and described in Section 8 of this synthesis document. The broader Benefit-Cost Assessment also takes into consideration the potential security benefits of the FOT technologies. In examining only motor carrier efficiency, it should be noted that a number of the technologies are primarily security-oriented in nature, and do not necessarily create a measurable operational improvement through their use (i.e., Panic Buttons or E-seals).

Regardless of technology configuration in the FOT, two technologies create the enabling platform on which the other test technologies operate – Wireless Communications and asset positioning/tracking. Through discussions with the participating motor carriers, these two capabilities provide the majority of measurable operational benefits. Without these two capabilities, potential operational, as well as safety and security benefits of the other test technologies, could not be realized.

5.1.1   Definition of Benefits

Based on the information collected during the FOT, at the micro or carrier-level, benefits were accrued through closer management of assets and personnel. Better management reduced out-of-route miles, enhanced driver productivity by facilitating the monitoring of location and driver work status, and through dynamic routing, potentially realized the opportunities for additional loads. The core mobile communications and asset tracking enabled the motor carriers to monitor their fleet operations both in near real-time and through historic record analysis to set tighter performance measures, and to realign fixed and variable routing decisions.

5.1.2   Analyses

Due to differences in the types of operations represented by the four load types in the FOT, the following two distinct analysis types (described in detail in Sections 5.2 and 5.3 of this synthesis document) were used to assess potential benefits for the participants:

1. Input Factor Productivity, which allowed for determining increases in output for a given level of an input, or conversely, reducing the required level of input for a given output (i.e., increased number of pickups and deliveries for a given number of drivers).

2. Partial Budgeting (of revenue increases and cost decreases), which was based on examining only those line items that represent a change from a baseline environment. Specific to this analysis, only those cost and benefit streams directly associated with the technologies' ability to effect change were considered.

---

[7] SAIC, *Hazardous Material Transportation Safety and Security Field Operational Test Final Detailed Test Plans*, prepared for FMCSA, September 2003.

5.2   INPUT FACTOR PRODUCTIVITY

This approach establishes and monetizes input factor efficiency in terms of increased output, holding other inputs constant, which was considered an appropriate framework for the 1A-B Bulk Fuel and 2B LTL (Non-Bulk pick-up and delivery [P&D]) scenarios in which driver productivity is a key operational metric.

Two analyses were conducted using Input Factor Productivity techniques – one for Bulk Fuel and another for LTL-Non-Bulk type operations because the participating motor carriers supplied two distinct types of operational data. The two analyses are described in the following Sections 5.2.1 and 5.2.2.

5.2.1   Bulk Fuel Analysis

The motor carrier represented in Scenario 1 operates under contract to customers to deliver gasoline to stations within approximately a 2-hour drive form the terminal. The key driver performance metric is percent of on-time performance versus a target schedule developed based on historical trip times. This motor carrier closely monitors this performance on a weekly basis to manage the drivers' productivity. The higher the percentage of on-time occurrences, the more trips can be made in a given day, thus reducing marginal driver costs, and maintaining customer satisfaction. This means that the driver cost per delivery declines.

This motor carrier recently began using a Wireless Communications with GPS system to more accurately capture time-stamped events (start and end of day, breaks, arrive/leave rack, arrive/leave customer locations, etc.). The motor carrier provided the weekly performance statistics for 19 Bulk Fuel delivery drivers based at the main carrier terminal. These data covered an 11-week timeframe, beginning in mid-December 2003 (when the system was proved out and employees trained and familiar with the system). The weekly driver productivity reports demonstrated an overall increase in driver productivity over 11 weeks of 11 percent, bringing the aggregate level to approximately 90 percent of target. This level is seasonally adjusted to reflect varying operating demands throughout the year. This is considered a high level of utilization, but through monitoring and driver management efforts, the carrier continues to maintain and increase the level. Figure 5-1 presents weekly average driver productivity levels versus target for the 11-week period.

Given the relatively small sample size over a relatively short period of time, the statistical significance of the observed productivity gains was tested and shown to be statistically significant at the 95 percent confidence level. In other words, the observed gains in productivity are real and not the result of sampling error.

To impute a cost savings (benefit) of these productivity gains, the loaded driver cost for this industry segment of $21.24 per hour was used.[8] The calculation of driver cost savings is defined as follows:

> Percent Productivity Gain x Hourly Driver Cost x Hours Worked/month
> = Monthly Savings/Driver
> = 11% x $21.24 x 208 hrs/month
> = **$486 per driver per month**, or approximately **$5,800 per year**.

---

[8]This figure was derived from the USDOT Bureau of Transportation Statistics, Motor Carrier Finance and Operating Statistics, 2002, accessed from http://transtats.bts/gov.

This benefit estimate can be used as a per truck estimate, if one assumes one 8-hour shift per day. For those Bulk Fuel operations operating two shifts, the estimated per truck benefit can be doubled to **$972 per truck per month**.
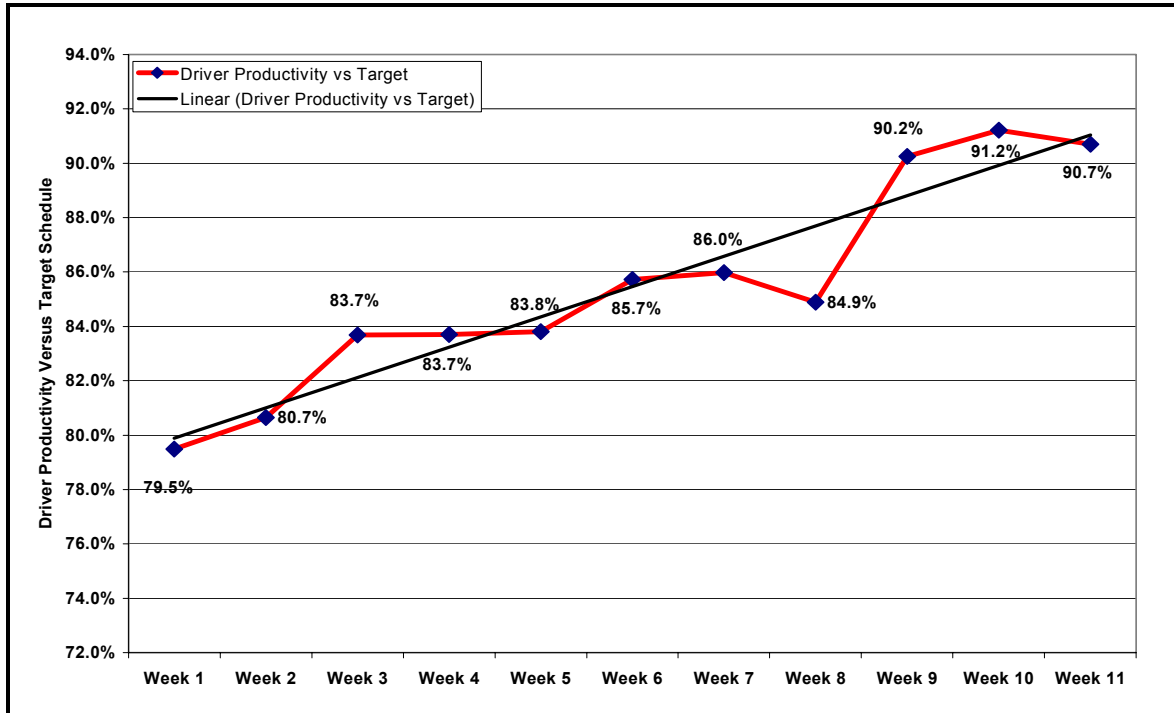
Figure 5-1. Average Bulk Fuel Driver Productivity Relative to Target Following Deployment of Wireless Communications and GPS Positioning Systems.

5.2.2 LTL-High Hazard (Non-Bulk) Analysis

The participating motor carrier in Scenario 2 began a phased approach to installing the Wireless Communications with GPS vehicle positioning system into its fleet on a terminal-by-terminal basis in 2000. The deployments are currently ongoing, and since the end of 2003, trucks at over 2,000 terminals have been equipped with Wireless Communications with GPS tracking.

For each phase of the deployment, the resulting changes in performance are normalized to a Year 0 and averaged across a taper for Years 1-3 following deployment. (Year 3 is the last year where at least two "deployment class years" are represented.) This was done to account for any potential "learning curve" or adoption/productivity initial impacts that may exist. Additionally, a "non-technology" sample of terminals was available from the motor carrier to provide a "without" baseline for comparison purposes.

The net gains represent the difference between the driver productivity (as defined by pounds per hour picked up and delivered while on duty) for the "technology-equipped" terminals and those without the technology. By Year 3, average pounds per hour for the terminals with Wireless Communications with GPS vehicle positioning equipped trucks were 3.5 percent higher than for those terminals with trucks not equipped. Closer management of driver en-route activities (monitoring of driver downtime), improvements in dynamic routing decisions

based on known vehicle positions are the primary contributory factors in realizing the improvement.

To impute a cost savings (benefit) of these productivity gains, the loaded driver cost for this industry segment, the same methodology was used as for the Bulk Fuel scenario. The value of these driver productivity (P&D) gains is calculated as:

    3.5% net P&D increase x $26.42 avg. loaded driver wage/hr. x 173 hrs
    = **$160** per driver per month, or **$1,920 per driver per year**.

If one assumes one 8-hour shift per day (which is conservative, considering LTL shifts can run up to 10 hour days), then the per truck benefit would be **$160 per month**. Table 5-1 presents the yearly driver productivity gains.

Table 5-1. Average LTL (P&D) Driver Productivity Gains Following Deployment of Wireless Communications and GPS Positioning Systems

Year	Net Increase in Driver Productivity
Year 1	2.3%
Year 2	3.4%
Year 3	3.5%

5.3   PARTIAL BUDGETING

The second approach that examined the impacts of technology on operations uses a framework that specifically examines the impact of technology on:

- Increased driver to dispatcher ratios.

- Reduced on the road delays.

- Reduced fuel consumption.

- Reduced out-of-route miles.

This modeling framework, best suited for operations approximating line haul, was found to be appropriate in assessing ROI for the following scenarios: 2A LTL-High Hazard; 3A-C Bulk Chemicals; and 4A-B Truckload Explosives.

The inputs were derived from carrier-provided operational and financial data, as well as anecdotal information, detailed analysis of archived data for the test trucks, and from published sources.

As the participating motor carriers have been using the Wireless Communications with GPS vehicle positioning for several years on a fleet basis, little "non-technology" baseline data was available to make direct before and after or with and without comparisons. The Evaluation Team used the companies' operating parameters, with participant opinions to model what the likely impacts on ROI would likely be if deployed currently. The opinions, albeit anecdotal, did benefit from this prior experience. Very conservative estimates of potential new load opportunities were used in the input set, recognizing that often, HAZMAT hauls are dedicated runs with specialized equipment and cannot always take advantage of a revenue producing backhaul as might be possible in dry van operations.

5.4   PARTIAL BUDGET ASSUMPTIONS, INPUTS, AND RESULTS

The inputs used in calculating per truck monthly benefits of Wireless Communications with GPS tracking are presented in **Volume III, Section 2**. The ROI model essentially equates downtime savings associated with eliminated driver call-in stops and unscheduled en-route maintenance/repairs with increased asset capacity. The ability to know where assets are, the state of conditions vis-à-vis maintaining schedule, and knowing driver availability for hours of service allows dispatchers/load planners to assess the feasibility for picking up potential backhaul loads (applicable to the operation). The model also estimates the value of freed up phone call time for dispatchers talking with drivers, thus allowing them to focus on other duties, or have the time to manage more drivers if necessary. Other benefits include lower communications costs, less idling time (associated with driver call-in stops), resulting reduced in fuel and engine wear costs. These benefits are displayed in Table 5-2.

As described, the inputs are conservative in terms of the percent of additional full loads (no partial loads are assumed) that can be realized (1percent), or the percent of non-productive miles that can be eliminated (1percent). Therefore, the benefit estimates are relatively conservative.

**Table 5-2. Estimated Monthly Per Truck Benefits Derived Using
Wireless Communications with GPS Vehicle Positioning System**

BENEFITS	LTL-High Hazard	Bulk Chemicals	Truckload Explosives
REDUCED CALL STOPS / CHECK CALLS	**$296**	**$253**	**$491**
• Reduces Telecommunications Costs	$28	$19	$30
• Increases the number of trucks dispatchers handle	$165	$122	$81
• Increases potential number of loads	$27	$37	$290
• Reduces idle time fuel consumption	$65	$65	$78
• Reduces idle time engine wear	$11	$11	$13
IMPROVED MAINTENANCE SCHEDULING	**$36**	**$18**	**$37**
• Reduces maintenance and repair costs	$33	$17	$33
• Increases revenue miles by reducing repair down-time	$2	$1	$4
REDUCED OUT-OF-ROUTE MILES	**$180**	**$123**	**$116**
• Creates savings of line haul variable costs	$180	$123	$116
IMPROVED VEHICLE UTILIZATION BY REDUCING EMPTY MILES	**$309**	**$199**	**$270**
• Increases potential number of trips	$309	$199	$270
TOTAL MONTHLY BENEFIT PER TRUCK	**$820**	**$593**	**$914**

A sensitivity analysis of benefits was conducted on the variables given the assumptions that a percentage of out-of-route miles can be eliminated through improved trip monitoring, or the percentage of added trips that could be hauled with better pre-planning and fleet utilization (both of which strongly impact monthly benefits per truck) would be increased.

LTL-High Hazard operations (as represented by the motor carrier in scenario 2B) with a 1 percent reduction in out-of-route miles or a 1 percent increase in monthly trips would increase monthly benefits by $180 and $309 per truck per month, respectively. For Bulk Chemicals, the benefit increases are estimated to be $116 and $270, respectively. For Truckload Explosives, the benefit increases by $124 and $199, respectively.

The potential benefit increases for a 1 percent reduction in out-of-route miles are calculated to be 21, 20, and 14 percent for LTL-High Hazard, Bulk Chemicals and Truckload Explosives, respectively. A 1 percent increase in loads hauled is calculated to increase benefits by 38, 46, and 22 percent for LTL-High Hazard, Bulk Chemicals, and Truckload Explosives, respectively.

The results of the sensitivity analysis show that even marginal improvements in managing out-of-route miles or improving asset utilization as reflected in increased loads hauled can have a strong effect on carriers' profitability and ROI.

It is recognized that all operations are not able to realize many of the estimated benefits as modeled for the FOT participants. The proportion and degree to which carriers realize benefits of technologies has been examined in numerous case studies and industry benefit/cost analyses. To explore low-end benefits of the Wireless Communications with GPS vehicle positioning system, this effort draws upon the results of a 1999 ATA Foundation study that examined the benefits and costs of technology systems across a wide-range of carrier operations for over 900 surveyed motor carriers.[9] Among the findings, carriers using Wireless Communications and vehicle tracking technologies, 33 to 47 percent increased loads; 22 to 35 percent reduced non-revenue miles; and 12 percent lowered driver to dispatcher ratios.

By focusing only on these three areas of operational efficiency improvements (using the midpoint values) and ignoring the other modeled benefits, the results of a "minimum" benefit analysis is presented in Table 5-3.

---

[9] *Motor Carrier Technologies – Fleet Operational Impacts and Implications for Intelligent Transportation Systems/ Commercial Vehicle Operations*, ATA Foundation, October 1999, conducted for Federal Highway Administration.

Table 5-3. Minimum Estimated Monthly Per Truck Benefits Derived through the Use of Wireless Communications with GPS Vehicle Positioning System.

BENEFITS	LTL-High Hazard	Bulk Chemicals	Truckload Explosives
REDUCED CALL STOPS / CHECK CALLS	**$20**	**$15**	**$10**
• Increases the number of trucks dispatchers handle	**$165 x (12% of fleets) = $20**	**$122 x (12% of fleets) = $15**	**$81 x (12% percent of fleets) = $10**
REDUCED OUT-OF-ROUTE MILES	**$52**	**$36**	**$34**
• Creates savings of line haul variable costs	$180 x (29% of fleets) = $52	$123 x (29% of fleets) = $36	$116 x (29% of fleets) = $116
IMPROVED VEHICLE UTILIZATION BY REDUCING EMPTY MILES	$124	$80	$108
• Increases potential number of trips	$309 x (40% of fleets) = $124	$199 x (40% of fleets) = $80	$270 x (40% of fleets) = $108
TOTAL MONTHLY BENEFIT PER TRUCK	**$196**	**$130**	**$152**

5.5   EFFICIENCY BENEFITS FINDINGS

A key finding was that the participating motor carriers ascribed little operational efficiency impact to the test technologies, with the exception of Wireless Communications with GPS tracking capabilities. Their views regarding operational efficiency were primarily focused on the ability to communicate efficiently with drivers, know where the vehicles are, and when to manage customer requests for status and arrival times; track driver and vehicle operational performance on the road; and to effect better load planning.

The use of Wireless Communications with GPS tracking capabilities shows significant benefits in terms of improved management of fleet personnel and assets to reduce unproductive miles; increase driver and dispatcher productivity; and realize increased loads.

There may be minimum fleet sizes in these sectors under which the usefulness of integrated communications and tracking systems may be easily reproduced with less advanced methods and technologies, such as cell phones and pagers. **Volume III, Section 4: Benefit-Cost Assessment and Industry Deployment Potential** examines this in the larger industry context.

Though not quantified through this effort, several of the participants thought GPS tracking was a valuable tool in the recovery of stolen assets – especially tractors and trailers. With the value of a tractor-trailer combination unit worth in excess of $100,000 and the cargo considerably more, being able to track and locate a missing asset is considered a potential ROI improvement, albeit, not quantifiable to the extent of rigor.

Geofencing was thought of as a useful application of the vehicle tracking system to enable alerts if a driver went out of route, thereby potentially reducing the costs of out-of-route miles. The efficiency benefits of Geofencing were considered in the Partial Budget analyses presented in the preceding sections as supporting the reduction in out-of-route miles. The exposure of the technologies to tethered and untethered trailer tracking was limited during

the test and resulted in no significant quantifiable benefits. Participants using the technologies did acknowledge that benefits could include reduced equipment abuse by third parties. They further acknowledged that this could result in reduced trailer maintenance and possible realization of detainage charges, reduced numbers of trailers needed to meet service needs, and potentially reduced staff/administrative costs associated with equipment matching and dispatching activities.

There may be minimum fleet sizes in these sectors under which the usefulness of integrated communications and tracking systems may be easily reproduced with less advanced methods and technologies, such as cell phones and pagers. **Volume III, Section 4** examines this in the larger industry context.

As mentioned previously, the ESCM concept was viewed as a potential efficiency tool through the reduction of paperwork. System use was constrained by the number of participants, and therefore, though the concept was accepted, reaction to the system itself was neutral.

The overall impact of the technologies on the motor carriers was that the technologies required the basic communications and tracking system, and that the carriers would realize additional costs in the concept of enhanced security. In this context, panic alerts and remote door locking capabilities were considered very useful with a willingness of carriers to possibly invest in them. For the most part, the participants indicated that the other "security" technologies would be considered, if the carriers' customers required their use and were willing to recoup the carriers' costs through increased freight rates.

6. SECURITY BENEFITS ASSESSMENT

The primary evaluation objective of the Security Benefits Assessment is to examine the ability of the test technology suites to improve HAZMAT shipment security. This objective is achieved by assessing the test technology suites' (and technologies with similar functionality available in the marketplace) in coordination with reasonable security processes and procedures to reduce the vulnerabilities in truck-based HAZMAT shipping, and thus, reduce the risk of successful HAZMAT-based terrorist attacks.

6.1   SECURITY BENEFITS ASSESSMENT OVERVIEW

Assessing the potential security impacts (consequence reduction) related to the HAZMAT FOT presented a significant evaluation challenge for two key reasons:

1.   There is little or no event data on which to reliably baseline the level of HAZMAT-based terrorist attacks or to provide actuarial data in which to predict a statistically significant number of actual terrorist actions in the future.

2.   A method needed to be developed that would translate field test performance and user acceptance information into monetized risk reduction terms.

Consequently, the Evaluation Team developed a unique analytical framework to assess potential benefits. This framework built upon traditional vulnerability assessment techniques, combined observations from both real-world and simulated operations within the FOT framework, and made use of expert judgment and sensitivity analysis. The core of this framework is expressed in a classic vulnerability assessment equation:

Threat x Vulnerability x Consequence = Cost

where "Cost" is the financial impact of HAZMAT-based terrorist attacks.

By applying this formula both before and after the deployment of technologies, it was possible to determine the likely security impacts of the test technologies and to express these impacts in quantifiable, economic terms.

To begin the technology benefits assessment, typical HAZMAT motor carrier operational scenarios were identified and the most likely terrorist attack profiles for each of these scenarios were developed. For example, a typical operational scenario may be the delivery of a bulk fuel. A possible associated attack profile for this load and shipment scenario may be the use of false manifest to divert this fuel shipment and delivery to a populated area for intentional release. The four key operational scenarios or load types considered under the FOT were: Bulk Fuel, Less-than-Truckload High Hazard, Bulk Chemicals, and Truckload Explosives.

A series of these operational scenarios and associated attack profiles were developed by the Battelle Deployment Team and have been documented in earlier reports.[10] These scenarios

---

[10]Battelle, *HAZMAT Field Operational Test Task One: Conduct A Risk/Threat Assessment*, Draft Report prepared for the U.S. Department of Transportation (USDOT), Federal Motor Carrier Safety Administration (FMCSA), October 2002. Also, from Battelle, *Framework for Assessing Safety & Security Incident Consequences for Highway Shipments of Hazardous Materials*, Final Report, prepared for the USDOT and FMCSA, December 2003.

and profiles also formed the basis for the FOT deployment of technologies.[11] An example of such a scenario would be the theft of a fuel truck while en route, driven to a populated area, and detonated to maximize casualties.

Once the operational scenarios and attack profiles were established, determinations of the extent of the *threat*, or the probability that a given attack scenario may be attempted were made. This value is a function of terrorist aims and operating procedures. Through discussion amongst the Deployment Team, FMCSA, and the Evaluation Team, threats are not expected be impacted by the technologies deployed in this HAZMAT FOT. Deployment of a technology or set of technologies may make a given attack scenario less desirable relative to others, but the technology would not alter the terrorist overall desire to inflict harm. Therefore, *threat* is held constant throughout this assessment. Furthermore, as the war on terrorism continues, it is anticipated that the overall threat environment will not be held constant. Should this become the case, the analytical framework presented here can be easily adjusted to reflect such a revised threat environment.

Having established threat values, it was necessary to determine weight and rank of *vulnerabilities*. These vulnerabilities represent the probability that a given attack profile will be successful, given potential weaknesses in the various stages and processes involved in transporting HAZMAT from shipper to consignee. Vulnerabilities may include physical security gaps, information integrity lapses, operations failings, and environmental factors that are favorable to terrorist goals. These vulnerabilities were defined by the Deployment Team and consolidated into higher-level categories, described in Section 6.2. Once the "before" vulnerabilities were assessed, the Evaluation Team determined the impact of the FOT technologies to address the vulnerabilities.

Should vulnerabilities be exploited, it is critical to next determine the likely *consequence* of a success for a given attack profile and HAZMAT operational scenario. For this study, the consequence estimates represent aggregate numbers that include societal impacts – lost wages, damage to infrastructure, and loss of human life – as represented by economic values. Again, these values were determined in a previous effort performed by the Deployment Team for the FMCSA.

As with the threat element of the vulnerability assessment formula, the consequence of a successful attack was considered to not change as a result of the technology deployment.

The final activity in the benefits assessment framework was to establish the potential number and type of terrorist attacks expected over the time horizon of 3 future years. Using these incident occurrence estimates with per incident consequence dollar value and the vulnerability reduction estimates, overall reduction in potential impacts (benefits) were estimated for each considered technology countermeasure for each load type.

The Evaluation Team utilized two distinct groups of subject matter experts in developing the Security Assessment framework: an *Expert Panel* and a *Delphi Panel*. These two panels further provided input to derive the initial vulnerability values, the potential technology-enabled vulnerability reductions, and the likelihood of attacks using truck-based HAZMAT shipments. It should be emphasized that the estimates of vulnerability made by the Delphi

---

[11] On the basis of the Deployment Team's initial Threat/Risk Assessment, load/operational types were prioritized with four type chosen for the FOT: Bulk Fuel; Less-than-Truckload-High Hazard Materials; Bulk Chemicals; and Truckload Explosives.

Panel were based on the Panelists' personal domain knowledge and information provided to them on technical performance and user acceptance/issues. The information provided to the Panelists was derived through the FOT via Beta and interim technology tests, conducting staged security violation events, and through before and after interviews with test participants. These inputs are well documented in **Volume III, Section 2: HAZMAT FOT Technical Performance, Efficiency and Safety Benefits Assessments**.

The Expert Panel is a core advisory group consisting of 16 project-sponsored or volunteer experts in HAZMAT transportation, national security, risk and loss prevention, and public safety. Through the Expert Panel, the assessment benefited from the inputs and guidance provided by representatives of the American Trucking Associations (ATA); the National Tank Truck Carriers Association (NTTCA); the Commercial Vehicle Safety Alliance (CVSA); International Association of Chiefs of Police; International Association of Fire Chiefs; motor carriers; insurance companies; USDOT; the U.S. Transportation Security Administration (TSA); and the Deployment Team.

The Evaluation Team coordinated with the Expert Panel through dissemination of background and follow-up materials, Web-Ex-based conferences, and on-site meetings. These coordinated efforts resulted in developing and refining the initial risk assessment assumptions and ranges of impacts for inclusion into an iterative Delphi Method.[12] The assessment framework was approved by the Expert Panel, which also assisted in identifying and recruiting participants for the larger Delphi Panel of experts discussed below.

Using the Delphi Method has become a widely used practice regarding transportation vulnerability assessment[13] due to the complexity of the interactions between factors and the wide range of estimates on the effectiveness of any assessed technology or strategy. Through the use of a Delphi Method, experts were asked to provide estimates of vulnerability and of the beneficial effects of the FOT-considered technologies. These inputs were collected via surveys. Both numerical and linguistic responses were developed over a series of group interrogations. Outputs with linguistic values were then processed using Soft Computing Methods in order to provide input values that support conventional Multi-Attribute Decision Making Methods.[14]

The Delphi Panel supporting this assessment was comprised of 26 expert individuals, either familiar to the members of Expert Panel, and/or previously identified through their affiliation with associations, conferences, or working groups (notably the FMCSA HAZMAT Working Group), which was recruited to support this effort. The Delphi Panelists were highly knowledgeable experts in the subject of security, risk assessment, emergency response, and enforcement as pertaining to HAZMAT shipping. The panel was comprised of the following mix of representatives:

- HAZMAT Motor Carriers (10)

---

[12] The Delphi Method provides a technique to arrive at a group position regarding an issue under investigation. This method consists of a distributing a series of repeated interrogations, usually as questionnaires, to a group of individuals whose opinions or judgments are of interest. After the initial interrogation of each individual, each subsequent interrogation is accompanied by information regarding the preceding round of replies, usually presented anonymously. The participant is encouraged to reconsider, and if appropriate, to change a previous reply in light of the replies of other group members. After two or three rounds, the group position is determined by averaging the responses. The Delphi Method was originally developed at the RAND Corporation by Olaf Helmer and Norman Dalkey.

[13] The Volpe Center, *Surface Transportation Vulnerability Assessment*, October 25, 1999.

[14] Evangelos Triantaphylou and Chi-Tun Lin, *Development and Evaluation of Five Multi-Attribute Decision Making Methods*, International Journal of Approximate Reasoning, 1996, Volume 14, pp. 281-310.

- Enforcement-State Police (3)

- Fire Fighters (4)

- HAZMAT Shippers/Manufacturers (5)

- Insurance/Risk Management (4)

Through three distinct surveys, these experts provided their opinions on pre-technology vulnerabilities, the impacts of technology to reduce the vulnerabilities, and the likelihood of truck-based HAZMAT attacks. These opinions were derived through an iterative process through which opinions were fed back to the Panelists anonymously, allowing individuals to reconsider their responses independently. This approach led to a movement of responses towards consensus, with the underlying reasons for minority positions documented.

Initially, the Evaluation Team briefed the Panelists with an overview regarding the FOT and the need for and overall purpose of the exercise and the Delphi process. This provided the Panelists with the base information to estimate the relative weighting of vulnerabilities and attack types for the four load types represented in the FOT.

Once the baseline vulnerability scores were established via the first survey, the Panelists were presented with detailed descriptions for the FOT technologies and deployment scenarios. The panel also received preliminary FOT results of technical and institutional performance for the test technologies. This aided the Panelists in developing their opinions (via the second survey) on the relative reductions in vulnerabilities through the use of the technologies.

The derivation of vulnerability weightings and the potential beneficial impacts of technology on risk, were based on the consensus of opinion of the 26 experts. However, residual variability in the Panelists' responses, following iterative interrogations, was accounted for in the final calculation of technology-enabled reductions in risk through the use of Monte Carlo simulation techniques. The Monte Carlo simulations consider the variability around input estimates (relative weighing of risk factors and the impacts of technologies on the risk factors) and provided solutions described by probability functions. These functions enabled potential security benefits to be presented in ranges across the probability functions.

Figure 6-1 presents an overview of the security assessment process.
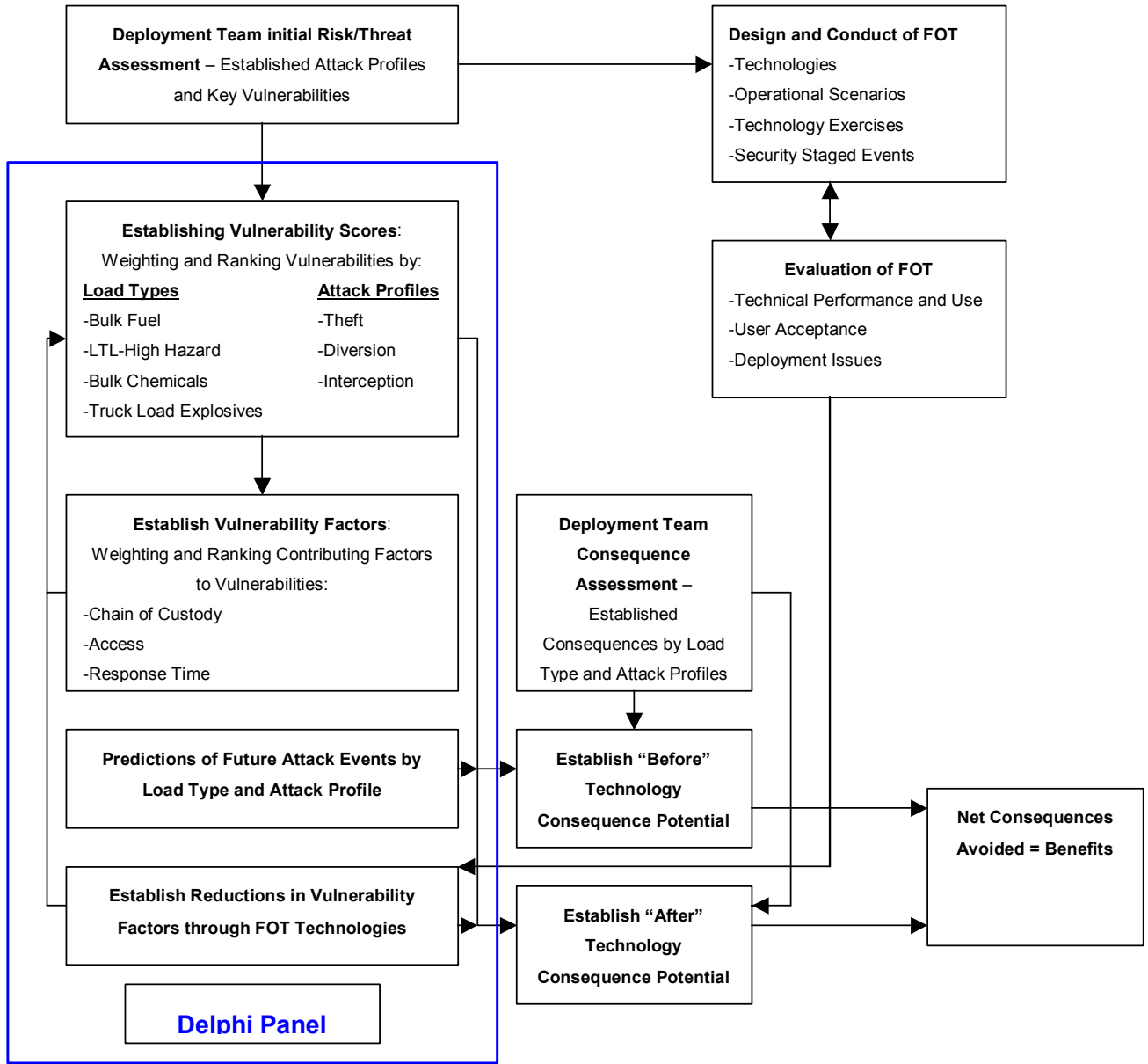
Figure 6-1. Security Assessment Process.

6.2   VULNERABILITIES AND TECHNOLOGY-ENABLED VULNERABILITY REDUCTIONS

As defined by deployment Task 1 of the FOT, the following three attack profiles were considered by the Delphi Panel for each load type:

- *Theft* is undertaken by means of stealth, deception, or force. Stealth and deception are deterred by detection, while force assumes detection and operates within parameters defined by the time to communicate and mount an interdiction. Stealth, deception, and force also define an escalation path for operational planning purposes.

- *Diversion* is a tactic that results in either theft or interception. The purpose is to create a path to a target opportunity or arrive at a location where control of the cargo by the terrorists can be achieved.

- *Interception* is the "instantaneous" version of theft in that the cargo is released and/or detonated, and ignited while still in control of the shipper/carrier/consignee. Particularly effective when the radius of damage is large, this is potentially the most violent of attack profiles in that it likely involves explosives as the mechanism for effecting material release.

Contributing to the potential success of an attack, three Vulnerability Factors (*VF*) were evaluated by the Delphi Panel:

- *Chain of Custody* – Protection of the Chain of Custody (CoC) is the ability to ensure that a shipment is in authenticated hands during the entire transportation process. CoC represents the first line of defense allowing positive tracking of the material form the point of origin to the point of delivery. Each shipment type infers a set of procedures that are followed at points where custody must affirmed or transferred.

- *Access* – If an attacker is unable to gain access by intercepting the CoC, this individual may elect to take forcible measures to gain control of the shipment and acquire access. Access is the ability to get inside of a critical effects perimeter (CEP) on the asset given that it has been identified and intercepted. The CEP is different depending on the threat. For detonation in place, this perimeter can be thousands of feet; for theft, the perimeter may involve cab entry. Access is measured as the probability that the adversary will get inside the CEP for a given shipment type and given threat.

- *Response Time* – Response time is the timeframe that it takes for authorities to identify that a shipment has been seized, mobilize response forces, close on the asset, and to neutralize the consequence potential. Response time is a function of the level of monitoring, the location and alert posture of response forces, and the ability to track the asset once it has been commandeered.

In establishing the "before" or "no technology" baseline, the Delphi Panel was surveyed to evaluate the vulnerability of each shipment type against each attack type in a structured format. The panelists assigned a *Vulnerability Score (VS)* to each of the shipments considered in the FOT for each attack type. The panelists were asked to assign a value in a range using a rating scale from 0.0 to 10.0 (in which 0.0 is extremely low and 10.0 is extremely high). This value, the *VS*, served three purposes to:

- Establish the vulnerability for a shipment to an attack type (theft, diversion, or interception).

- Establish the Panelists' estimate of the relative vulnerability among all shipment types to a particular attack type.

- Establish the Panelists' estimate of the relative severity among threats.

The Panelists then estimated the contribution of each *VF* to the *VS* for each shipment type. This is done by assigning a "weight" (in terms of percentage) to each *VF* (chain of custody, access, and response time), indicating the Panelists' judgments on the degree of influence each factor has on the overall vulnerability of a shipment type to a specific attack type. The Panelists' judgments are made based on evaluation of the baseline information, or pre-technology condition.

The before (no technology) and after (with technology) impacts of technology on these Delphi Panel-weighted vulnerability factors were incorporated into overall probability of attack success reductions. The weighted sum mean reductions in probability of success for each of the attack types, by load type, and by technology countermeasure, are presented in Tables 6-1 through 6-3, respectively. These were derived by averaging the technology-enabled reductions in vulnerability of the contributing **VFs**, weighted by the contribution of each **VF** to the attack types.

The relative likelihood of attack methods and the weighting of vulnerabilities/vulnerability subcomponents assigned to the load types by the Delphi Panel were used to develop overall vulnerability reduction for the technologies by load type These are average vulnerability reductions weighted by the **VSs** for each load type. These are presented in Table 6-4 and Figure 6-2.[15] *The significance of the overall vulnerability reduction is when multiplied by the potential consequences of attacks using HAZMAT, provides an estimate of potential security benefits afforded by the technologies.* The potential security benefits are calculated in Section 6.3 of this synthesis document.

Table 6-1. Percent Reduction in Vulnerability of Theft by Load Type

Technology Countermeasure Scenarios	Bulk Fuel	LTL-High Hazard	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC)	23%	17%	19%	17%
WC + GPS Position	26%	24%	27%	20%
Panic Alert + (WC + GPS Position)	42%	37%	42%	33%
Driver ID + (WC + GPS Position)	40%	38%	39%	29%
Vehicle Disabling (+WC + GPS)	42%	39%	44%	31%
Cargo Seals (+WC + GPS Position)	NA	37%	NA	29%
Cargo Door Locks (+WC + GPS Position)	NA	36%	NA	29%
PSRC (WC + GPS Position)	37%	36%	39%	31%
ESCM (WC + GPS Position)	41%	39%	39%	29%
Panic Alert + Vehicle Disabling (+WC + GPS)	52%	47%	52%	40%
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	58%	54%	57%	43%
Panic Alert + Driver ID + ESCM (WC + GPS Position)	57%	53%	55%	42%
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	53%	NA	42%
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	52%	NA	42%

Vulnerability reductions from 0-10 percent are considered nil; reductions from 11-25 percent are considered low; reductions from 26-50 percent are considered medium; and greater than 50 percent are considered a high reduction.

---

[15]In Tables 6-1 through 6-3, electronic cargo seals and remote door locks were considered to be impractical for Bulk Fuel and Bulk Chemical load types, therefore "NA" ("Not Applicable") is used.

Table 6-2. Percent Reduction in Vulnerability of Diversion by Load Type

Technology Countermeasure Scenarios	Bulk Fuel	LTL-High Hazard	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC)	14%	13%	11%	11%
WC + GPS Position	16%	15%	14%	13%
Panic Alert (WC + GPS Position)	26%	23%	23%	23%
Driver ID + (WC + GPS Position)	24%	23%	21%	19%
Vehicle Disabling (+WC + GPS)	25%	26%	24%	21%
Cargo Seals + (WC + GPS Position)	NA	23%	NA	19%
Cargo Door Locks (+WC + GPS Position)	NA	22%	NA	19%
PSRC (WC + GPS Position)	24%	23%	22%	22%
ESCM (WC + GPS Position)	24%	24%	21%	19%
Panic Alert + Vehicle Disabling + (WC + GPS)	31%	31%	29%	27%
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	34%	34%	31%	29%
Panic Alert + Driver ID + ESCM + (WC + GPS Position)	34%	33%	30%	29%
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals + (WC + GPS Position)	NA	33%	NA	28%
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks + (WC + GPS Position)	NA	33%	NA	29%

Vulnerability reductions from 0-10 percent are considered nil; reductions from 11-25 percent are considered low; reductions from 26-50 percent are considered medium; and greater than 50 percent are considered a high reduction.

Table 6-3. Percent Reduction in Vulnerability of Interception by Load Type

Technology Countermeasure Scenarios	Bulk Fuel	LTL-High Hazard	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC)	7%	5%	5%	6%
WC + GPS Position	8%	6%	6%	7%
Panic Alert (WC + GPS Position)	12%	8%	9%	12%
Driver ID + (WC + GPS Position)	11%	8%	8%	9%
Vehicle Disabling (+WC + GPS)	11%	9%	10%	10%
Cargo Seals (+WC + GPS Position)	NA	8%	NA	9%
Cargo Door Locks (+ WC + GPS Position)	NA	8%	NA	10%
PSRC (WC + GPS Position)	12%	9%	10%	11%
ESCM (WC + GPS Position)	11%	8%	8%	10%
Panic Alert + Vehicle Disabling + (WC + GPS)	14%	11%	12%	14%
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	15%	12%	13%	14%
Panic Alert + Driver ID + ESCM + (WC + GPS Position)	15%	11%	12%	14%
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	11%	NA	14%
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	11%	NA	14%

Vulnerability reductions from 0-10 percent are considered nil; reductions from 11-25 percent are considered low; reductions from 26-50 percent are considered medium; and greater than 50 percent are considered a high reduction.

**Table 6-4. Percent Reduction in Overall Vulnerability
by Load Type and Technology**

Technology	Bulk Fuel	LTL-High Hazard	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC)	15%	13%	12%	11%
WC + GPS Position	17%	16%	16%	12%
Panic Alert + (WC + GPS Position)	27%	25%	25%	21%
Driver ID + (WC + GPS Position)	25%	25%	23%	18%
Vehicle Disabling + (WC + GPS)	26%	27%	26%	19%
Cargo Seals + (WC + GPS Position)	NA	25%	NA	18%
Cargo Door Locks + (WC + GPS Position)	NA	24%	NA	18%
PSRC (WC + GPS)	24%	25%	24%	20%
ESCM (WC + GPS)	25%	26%	23%	18%
Panic Alert + Vehicle Disabling + (WC + GPS)	32%	32%	31%	25%
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	36%	37%	34%	27%
Panic Alert & Driver ID + ESCM (WC + GPS Position)	35%	36%	33%	26%
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	36%	NA	26%
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	35%	NA	26%

Vulnerability reductions from 0-10 percent are considered nil; reductions from 11-25 percent are considered low; reductions from 26-50 percent are considered medium; and greater than 50 percent are considered a high reduction.
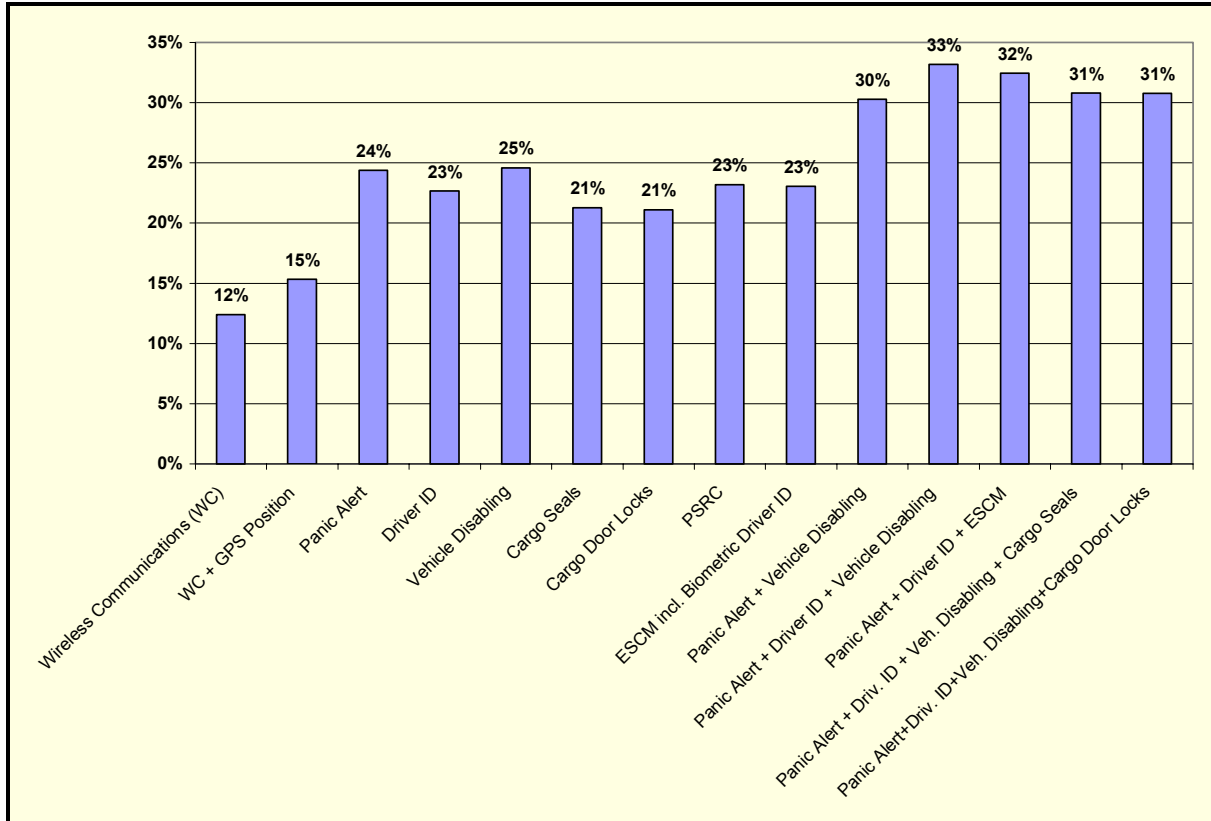
Figure 6-2. Average Percent Reduction in Overall Risk Across Load Types by Technology Combination.

6.3   SECURITY BENEFITS

For the Security Assessment, benefits were defined as potential reductions in the costs (consequences associated with HAZMAT-based terrorist attacks multiplied by the number of attacks) through full deployment of the technologies. These represent societal benefits. The "per event" potential consequences of HAZMAT-based attacks were obtained from a document developed by Battelle for FMCSA that explored the potential economic impacts of intentional and non-intentional releases of HAZMAT. The study examined the potential consequences as measured by:[16]

- Fatalities and injuries.

- Property Damage: Damage to the truck, to other involved vehicles, and to other public and private property.

- Product Loss: Quantity and value of the HAZMAT lost during a spill.

- Environmental damage.

- Evacuation: Predominantly short-term relocation of people and business operations.

- Cleanup: Stopping the spread of a release and removing spilled materials.

---

[16]*Framework for Assessing Safety & Security Incident Consequences for Highway Shipments of Hazardous Materials*, Final Report, Battelle, prepared for the USDOT and FMCSA, December 2003.

- Traffic Delay: Additional travel time experienced by the motoring public due to delays caused by the incident.

- Business Disruption: Businesses having to reduce or cease operations because the facility is inaccessible, supplies cannot be received, or other constraints imposed by the incident.

The estimates of the consequences of intentional releases of HAZMAT were derived through a framework that developed a series of multipliers to estimate the overall economic impacts of HAZMAT releases based on likely numbers of human casualties. The multipliers were based on a proxy measure for estimating effects. As the study states:

> Fires were considered a reasonable proxy in that a large-scale hazardous materials incident often includes a fire and/or explosion, affecting multiple residences/businesses and resulting in traffic delays and community disruption.[17]

Using these multipliers with estimated casualties for intentional HAZMAT releases based on load type, quantity and attack scenarios, reasonable worst-case consequence estimates were developed.

The Battelle study presented reasonable worst-case consequence estimates for nine threat-based classes of HAZMAT, four of which are used in estimating potential impact reduction in this assessment. Derivation of the per event consequence values used in this assessment considered the composition of HAZMAT for each load type, potential quantities released (TL versus LTL) and the Delphi Panel predicted distribution of attacks with undirected versus directed (including detonation) releases. Table 6-5 presents the per-attack consequence estimates used for this assessment.[18]

Table 6-5. Reasonable Worst-Case Per Attack Consequences

HAZMAT FOT Load Type	Reasonable Worst-Case HAZMAT Attack Consequences
Bulk Fuel	$3.7 Billion
LTL High-Hazard	$2.1 Billion
Bulk Chemicals	$16.3 Billion
Truckload Explosives	$13.3 Billion

To put these consequence numbers into context, the following examples of the consequences of terrorist attacks in the United States are proffered.

---

[17]*Framework for Assessing Safety & Security Incident Consequences for Highway Shipments of Hazardous Materials*, Final Report, Battelle, prepared for the USDOT and FMCSA, December 2003.

[18] Per event consequence estimates based on weighted averages of Delphi-predicted attacks by attack profile (directed release versus undirected release) and the following load types:

– Bulk Fuel – average of flammable liquids and flammable gases – Bulk quantity.

– LTL – heavier than air PIH in LTL quantity (LTL impacts estimated at 6 percent of TL or bulk impacts).

– Bulk Chemicals – heavier than air PIH in Bulk quantity.

– Truckload Explosives – sensitive explosives in Bulk quantity.

Two tragedies provide examples of the harm that can occur from explosive material delivered in a van or light truck: the 1993 New York World Trade Center (WTC) and the 1995 Oklahoma City Federal Building:[19]

- The 1993 WTC bombing killed six people, injured over 1,000, and resulted in over $113 million in loss of life and bodily injury, and over $510 million in insured losses (based on figures from the Federal Emergency Management Agency). Total losses are estimated to be $623 million.

- The Oklahoma City bombing killed 168 people, injured 601, and resulted in $560 million in loss of life and bodily injury, and over $125 million in insured losses. Total losses are estimated to be $685 million.

Vehicles used in the transportation of hazardous materials typically have much larger capacities than the vehicles used in these two incidents. If these vehicles were used to carry out a terrorist act, the damage would have been far worse. If certain hazardous materials were involved and released in a directed attack, it could result in far greater numbers of casualties and damage to property over a larger area.

Another example of the impacts of directed attacks in the United States, albeit attack(s) using airplanes against buildings as opposed to trucks, is the September 11, 2001 attack(s) on the WTC.

- The Government Accounting Office (GAO) reviewed eight studies from seven organizations that examined the financial impacts of the 9-11 attack on the World Trade Center.[20] The GAO concluded that the study conducted by the New York City Partnership and Chamber of Commerce provided the most comprehensive estimates: $83 billion in 2001 dollars for direct and indirect costs.

Although threat may vary over time and is difficult to predict, in estimating the security benefit, threat was held constant at 100 percent, meaning that there is a 100 percent chance that an attempt will be made to use a HAZMAT shipment for a terrorist attack. By holding threat constant, *the security benefits of the technologies were derived using, the overall vulnerability reductions* (presented in Section 6.2 of this synthesis document) *multiplied by the consequences of HAZMAT-based terrorist attacks*. For example, the benefit calculated for Wireless Communications with GPS positioning for Bulk Chemicals is calculated as follows:

(Bulk Chemical Consequence) X (Technology Vulnerability Reduction) = Benefit

= $16.3 Billion Consequence X 16% Vulnerability Reduction from Wireless Communications with GPS Positioning

= $2.6 Billion Benefit

The estimated security benefits are presented in Table 6-6**. *These figures are not additive across load types*.**

---

[19] Federal Register / Vol. 68, No. 86 / Monday, May 5, 2003 / Rules and Regulations, p. 23867.

[20] U.S. Government Accounting Office, GAO-02-700R, *Impact of Terrorist Attacks on the World Trade Center*, May 29, 2002. The reports that were reviewed were prepared by: the New York City Office of the Comptroller; New York Governor and State Division of the Budget; New York City Partnership and Chamber of Commerce; Fiscal Policy Institute; New York State Senate Finance Committee; Milken Institute; and, New York State Assembly Ways and Means Committee.

**Table 6-6. Estimated Security Benefits by Load Type and Technology
(In Millions of Dollars)**

Technology	Bulk Fuel	LTL	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$548	$268	$1,917	$1,409
WC + GPS Position (Baseline)	$622	$348	$2,581	$1,657
Panic Alert + (WC + GPS Position)	$995	$529	$4,058	$2,822
Driver ID + (WC + GPS Position)	$933	$537	$3,730	$2,345
Vehicle Disabling (+WC + GPS)	$970	$573	$4,278	$2,556
Cargo Seals (+WC + GPS Position)	NA	$529	NA	$2,345
Cargo Door Locks (+WC + GPS Position)	NA	$513	NA	$2,400
PSRC (+WC + GPS)	$908	$525	$3,891	$2,652
ESCM (+WC + GPS) incl. Biometric Driver ID	$946	$553	$3,730	$2,400
Panic Alert + Vehicle Disabling + (WC + GPS)	$1,207	$689	$5,098	$3,355
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$1,331	$776	$5,539	$3,547
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$1,318	$755	$5,319	$3,510
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	$755	NA	$3,469
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	$747	NA	$3,510

6.4 SECURITY ASSESSMENT FINDINGS

The field data collection and the risk-consequence assessment showed that the primary enabling technology combination on which all other technologies operated was Wireless Communications with GPS positioning. This combination is key to the security architecture deployed in the FOT. To assess the most widely used fleet management technology deployed (Wireless Communications) as a stand-alone application, the Delphi Panel was also asked to provide opinions on the beneficial effects of this technology. In framing the Delphi Panelists' responses, care was given to instruct them to assess the value of each technology independently, therefore, enabling a mix and match approach to technology combinations that could be used to model real-world deployment of technology suites across different load types/operations.

While the technology combinations do show promise for reducing the vulnerabilities of truck-based HAZMAT shipments, and thus, risk as expressed in reduced consequences, the Delphi Panel and the test participants provided a clear message that not all solutions are foolproof. Their responses also indicated that not all solutions perform to form in a dynamic real-world environment in which human and technology failures can occur, and where the adversary is cunning and looking for new ways to subvert security efforts. These opinions provide important discussion points for development of security-related public policy.

Following are the key findings derived from the Evaluation Team interaction with the Delphi Panel, which echoed the general comments provided by participating motor carriers:

- **Frequency in Driver/Dispatch Communication.** It was found that frequent communication with drivers and asset positioning are of significant security benefit. Inherent in the concept of asset positioning was the concept of Geofencing and Untethered Trailer Tracking. With user-configured polling frequency, these forms of communication types allowed dispatchers to know the whereabouts of their drivers and assets, and to be alerted in the event of crisis or exceptions to normal operational parameters.

- **Wireless Communications and GPS Positioning.** These items were considered vulnerable to possible electronic jamming and the ability of a driver to react and transmit a message while under attack.

- **Average Polling Rates.** The polling rates for GPS positioning were considered too infrequent to effectively track a vehicle, even at 20-minute average intervals.

- **Panic Alerts.** These items were considered valuable as reflected in the large incremental increase in vulnerability reduction, but may be limited in effectiveness for more local (within population areas) hauls where the damage could be done before intervention by enforcement. It was recommended that a driver-carried Panic Button be used in conjunction with in-vehicle Panic Buttons. Dissemination of panic notification should be via multiple modes (e-mail, fax, pager, cell phone, etc.).

- **Remote Vehicle Disabling.** This was also considered a strong vulnerability reduction technology, but it was recommended that it should be combined with driver-local disabling to be most effective, and not be solely reliant upon dispatcher trigger disablement. Additionally, concern was expressed over the reliability of the system to prevent a truck from being inadvertently stranded.

- **Driver Identification/Unit Assignment.** These were considered useful, but the human/technology relationship needed improvement (unobtrusive for the driver and more reliable). It was recommended that this technology be coupled with vehicle disablement to prevent unauthorized use of a truck.

- **Electronic Manifesting.** Acceptance was mixed, with comments focused on the potential system costs, complexity, and lack of a significant base of users as hindering factors.

- **Electronic Seals and Remote Door Locking.** These were considered useful for detecting tampering or providing a hard lockout until dispatch approves a door opening. These devices were not considered appropriate to Bulk Fuel and Bulk Chemical operations. Additionally the E-seal concept was not considered as mature as some of the other technologies; therefore reliability and potential cost were issues.

- **The Public Sector Reporting Center.** In concept, this item was considered as a strong vulnerability reduction system. In terms of identifying crisis and reducing response time, concerns exist about the potential frequency of false alarms/alerts that would burden public safety agencies, integration with existing systems such as computer-aided dispatch (CAD), and the potential cost of deployment.

7. SAFETY BENEFITS ASSESSMENT

The Safety Benefits Assessment framework for the FOT provided for the functional testing of 13 separate technology combinations across four load types. As described in **Volume III, Section 1: HAZMAT FOT Overview**, these technologies were designed to enable real-time communications and information exchange between drivers, dispatchers and other authorized parties; track assets; secure vehicles, loads and shipping documentation; and enable driver or automated exception alerts in response to crisis or deviations in operational characteristics outside of set parameters. The majority of technologies themselves and their usage are not specifically established to provide explicit or traditional safety benefits (i.e., reducing the frequency and severity of crashes). For example, the test technologies are not designed to warn drivers of obstacles in proximity to their vehicles, lane departure, imminent vehicle rollover conditions, or conditions signaling driver fatigue.

This notwithstanding, frequent driver/dispatcher communications allowing the dispatcher to assess the driver's condition and position tracking to assess possible driver speeding may equate to potential reductions in crashes. Additionally, a potential reduction in miles driven via tighter management of fleet operations enabled by Wireless Communications and GPS asset tracking capabilities may, be equated to reduced exposure to crashes.

The participating motor carriers and enforcement personnel have also described potential post-incident safety benefits by using several of the test technologies. Using Wireless Communications with GPS positioning, panic alert capabilities, and real-time information exchange with enforcement and response agencies can provide more immediate incident-alert notification; detect vehicle location; and identify the quantity and type of HAZMAT load on the distressed truck.

The benefits focus on the ability to more rapidly detect and respond to an incident with the most appropriate mitigating resources to a HAZMAT incident in a more timely and complete manner. Though mostly anecdotal in description, these benefits are considered realizable by HAZMAT stakeholders. It should be noted that six of the nine participating motor carriers either agree or strongly agree that the test technologies provide enhanced functionality for incident response.

The following analyses provides a high-level framework in which to assess the potential benefits of reduced crash exposure and improved response and treatment of truck-based HAZMAT incidents through the use of the test technologies.

The starting point for the analyses is a listing of relavent facts:

- Total Cost of HAZMAT truck crashes: $842 million per year.[21]

- The four load types considered in the FOT represent 67 percent of the recorded load types for trucks involved in fatal and non-fatal crashes in 2002.[22]

7.1   MOTOR CARRIER EXPOSURE TO CRASH ANALYSIS

In terms of reduced exposure to crashes, the test participants indicated a minimum reduction in out-of-route and empty miles of 1 percent through the use of Wireless Communications and GPS positioning. Depending on industry segment, this is a conservative reduction in

---

[21] FMCSA Analysis Division, Large Truck Crash Facts – 2002, 2001, 2000. Some estimates place this value as high as $1.1 billion per year. For the sake of conservatism, the lower number is used in calculation.
[22] Ibid.

non-revenue miles. ***Assuming this reduction of 1 percent represents a 1 percent in reduction in total miles traveled by carriers hauling HAZMAT***, then the benefit achievable (through full deployment) by reducing on-the-road exposure to crashes is calculated as:

> **$842 million per year (Total Cost of HAZMAT truck crashes) x**
> **1% (fewer miles/less exposure) x 67% of Crashes involving the FOT Load Types**
> **= $5 million in annual crash avoidance benefits**

7.2   ENHANCED HAZMAT INCIDENCE RESPONSE BENEFITS

As previously discussed, rapid notification of HAZMAT incidents with details of incident location and load type and quantity to motor carriers and emergency response organizations is widely considered necessary to maximizing the effectiveness of incident response and reduce the impacts of incidents. Difficulty in quantifying the potential benefits of the test technologies (focus being on the Public Sector Reporting Center [PSRC] concept, described in greater detail in Section 9 of this synthesis document) is due to all incidents being unique with regard to the following elements:

- Severity of event.

- Whether or not HAZMAT has been released.

- HAZMAT type and quantity involved in the incident.

- Travel routes.

- Time of day.

- Level of traffic on the route.

- Existing levels of roadway surveillance, agency communications capabilities.

- Availability of response resources with close proximity.

- Overall ability to coordinate the resources.

These factors make quantifying potential benefits of more rapid or appropriate response difficult at best. In other words, "No consistent standard has been identified that can be uniformly applied to evaluate the quantifiable benefits of an effective incident management program."[23]

This notwithstanding, safety benefits described extensively in the literature and by the FOT participants that can be achieved through improved incident response and treatment (that could be enhanced by the test technologies) include:

- Increased survival rate of crash victims.

- Reduced environmental mitigation costs and potential exposure of citizens to HAZMAT releases.

- Reduced incident-related congestion and hence, reduced occurrence of secondary accidents.

Though tested on a limited basis as a "proof of concept", the PSRC concept demonstrated a maximum of 2 minutes for a panic alert to be routed to law enforcement through the PSRC. As a comparison to the status quo, the Center for Technology Commercialization's "best estimate" of average notification time for state police response to a HAZMAT spill is 20 minutes, representing an 18-minute improvement in notification time.

---

[23] Kansas Department of Transportation, Incident Management Program Background, Spring 2002.

In terms of human life, emergency responders are well aware of the "golden hour." This refers to the chances for survival for a trauma victim being significantly greater if they receive emergency medical care within 1 hour of injury. In this context, the 18-minute decrease in notification time, assuming the driver was capable of triggering the panic alert, could potentially mean the difference between life and death for crash victims.

Additionally, the PSRC concept enables response organizations to know the location of the incident and rapidly access details on the type and quantity of HAZMAT involved in the incident to enhance response time and bring to bear appropriate mitigating resources, thus reducing the potential diliterious effects of a spill and reducing clearance time resulting in reduced congestion and potential occurance of secondary incidents.

7.3 SAFETY BENEFITS ASSESSMENT FINDINGS

The technical performance of the technologies within the framework of the FOT demonstrated enhanced ability to monitor drivers and vehicles and provide notification of emergencies with location and load characteristics in a more timely manner and potentially detailed manner than traditional methods. Though hard evidence is scarce, qualitative opinion indicates that the technical capabilities of the test technologies, coupled with best practices in motor carrier driver/safety management and public sector incident response, show promise for enhancing the safety of truck-based HAZMAT shipments.

Through the use of proxies, potential benefits in terms of crash avoidance were estimated to be $5 million annually. No monetized benefit estimates for enhanced emergency response were developed.

8. BENEFIT-COST ASSESSMENT AND DEPLOYMENT POTENTIAL

This section presents an overview of the processes of estimating the potential benefits and costs for the technologies and combinations of technologies tested during the FOT on a macro- and micro- (firm level) economic basis, and presents the finding regarding the market or full deployment potential for the industry.

8.1   OVERVIEW

8.1.1   Benefit-Cost Assessment

In **Volume III, Sections 2 and 3** present the security, operational efficiency and safety benefits that could be realized through the use of the technologies tested in the FOT. The security benefits were derived using FOT results in terms of the technical efficacy of the technologies. The benefits were also derived from the test participants' perceptions of the technologies and levels of potential consequence associated with the deliberate release or use of the hazardous materials associated with terrorist attack scenarios. This information was provided to a panel of industry experts (a Delphi Panel). The Panelists provided their opinions regarding relative risks and vulnerabilities; effectiveness of technologies to address the risks and vulnerabilities; and expectations of terrorist attempts in the near future to commandeer HAZMAT shipments and use them as weapons.

The processing of information to and from the Delphi Panel was conducted within a rigorous analytical framework that allowed for the derivation of macro, or societal, benefits (defined as reductions in potential consequences associated with HAZMAT-based terrorist attacks). These were developed for the four key load or operational types that comprise the majority and most at risk truck-based HAZMAT shipments.

Efficiency benefits – those benefits that accrue directly to the motor carriers – were calculated based on potential changes in operations due to the use of the FOT technologies. As described in **Volume III, Section 2**, few if any benefits were directly associated with the FOT technologies beyond the base enabling technology combination of Wireless Communications with GPS asset tracking. The calculated benefits were ascribed to improved asset and personal utilization and reduced communications costs. Anecdotally, participating motor carriers did view the ESCM as having the potential to augment their current freight tracking capabilities and reduce administrative costs associated with processing shipping documentation.

8.1.2   Industry Deployment Potential

The calculated macro-economic benefits and costs are directly related to the level of technology deployment by motor carriers hauling HAZMAT and are expressed over a range of potential deployment levels. Supporting the estimation of these macro-economic benefits and costs is the definition of potential market. Market (or full deployment) potential is defined in terms of the number of power units in each of the four load types that could be equipped with one or more technology combinations. Estimates of potential technology adoption by motor carriers and minimum acceptable return on investment periods is defined through the Deployment Team's motor carrier industry survey effort[24] and qualitative input from the motor carrier test participants regarding the financial attractiveness of the test technologies.

---

[24] ATRI, Trucking Technology Survey, conducted as part of the FOT, *Hazardous Materials Security and Technology Survey Results Summary*, January 2004.

Taken together, the aforementioned inputs provide a basis for defining the likely current level of technology deployment (with current levels of benefit versus an assumed baseline of no technologies), projected into the near future (3 years). The current and future levels of technology adoption, associated benefits, and costs are compared to the maximum or full deployment potential levels, with the gaps quantified.

8.2   INDUSTRY DEMOGRAPHICS

The Security Assessment and Efficiency Assessment provide system and motor carrier or shipment-level assessment of technology and procedural countermeasure efficacy. These efficacies were expressed by reductions in potential consequence(s) of HAZMAT-based attacks and profitability to motor carriers. To demonstrate the potential costs and benefits of motor carrier industry-wide adoption of the technologies, this assessment reduces the estimates to a per-truck basis, then extrapolates the security and efficiency findings to the universe of truck-based HAZMAT shipping in the United States.

This is done using demographic data on HAZMAT carriers documented in the FMCSA-maintained Motor Carrier Management Information System (MCMIS) Census File. MCMIS is a computerized system containing comprehensive industry demographic records (fleet sizes, load types, etc.). These records also contain safety performance records for the motor carriers and HAZMAT shippers who are subject to the Federal Motor Carrier Safety Regulations (FMCSR) or Hazardous Materials Regulations (HMRs).

The MCMIS Census file HAZMAT carrier-specific records were extracted and used to define the typology of the industry. Records were segregated for each HAZMAT class and division type, and shipment type (Bulk, Non-Bulk, or Bulk and Non-Bulk shipments). The fleet-specific data was aggregated by HAZMAT class, division, and shipment types into representations of the HAZMAT mix for the four load types being considered in the FOT. (In actually, there were five load types – LTL represents high-hazard shipments [Bulk and Non-Bulk type services]). These aggregations are detailed in **Volume III, Section 4**.

8.2.1   Industry Topology by Size

The numbers of trucks by load type formed the basis for establishing the per-unit benefits and costs and the full deployment potential. Within load type, the fleets were stratified based on number of trucks. This stratification was done to enable the assigning technology costs and potential for technology adoption most appropriate to the fleets – in general, smaller fleets are more capital constrained and often require a different technology mix for managing fewer assets. The fleet stratification was indifferent to the double counting of trucks across load types, as the assumed constraining factor to technology adoption is overall fleet size, regardless of specific loads.

Based on MCMIS, there are approximately 709,000 trucks associated with 26,760 U.S. fleets hauling HAZMAT in the four main load types. The demographics for the four operational segments for this FOT are covered in **Volume III, Section 4**.

8.2.2   Distribution of Fleets by Size and Relationship to Technology Adoption

As previously discussed, fleet size is related to the level of fleet management support technologies required to maximize operational efficiencies. For example, a fleet with only a few trucks and drivers would not likely require integrated communications, tracking, and decision support systems as would a fleet of 50 trucks or a fleet of 500 or more trucks would. In the case of small fleets, cell phones may be all that is needed to maintain driver-dispatcher

communications and establish current truck location. However, a larger fleet with greater demands on dispatchers may find the need for text messaging and vehicle tracking capabilities.

Across the four load types, approximately one-quarter to over one-third of the carriers is a one-truck operation. These one-truck operations require little, if any, technology above basic cellular or satellite phone services to support voice and Internet access for customer contact and load finding/bidding.

Fleets containing less than 10 trucks represent between two-thirds and over three-quarters of the HAZMAT haulers. As with the one-truck operations, methods of communications and fleet management are generally reliant upon low-cost solutions – mobile phone, two-way radio, and paging systems. Aside from the one-truck operations, there is potential for productivity improvements by adopting technologies (if priced at levels acceptable to small fleets) even in this universe of small operations.

Realizing the differing operational needs of fleets of different sizes and operational characteristics, the FOT fielded technologies in six different tiers of hardware, capabilities, and pricing per truck. Additionally, one FOT component was the development of a compendium of commercially available fleet management and security technologies of varying capabilities and pricing schemas that could provide affordable solutions for small fleets. These are discussed in detail in Section 5 of this synthesis document.

8.3   MOTOR CARRIER TECHNOLOGY ADOPTION

The motor carrier industry is a diverse collection of industries, with each responding to the unique demands of customers. Within each of these sub-industries or industry segments, there also exists a large amount of differentiation in how individual trucking companies operate and what portfolio of fleet management solutions (technical and non-technical) are used to conduct business. To support this diverse industry, a wide range of technology solutions are available to motor carriers, but not all commercial offerings are applicable to individual companies' operational needs or ability to pay for them.

Based on fleet size (a prime factor regarding levels of technology adoption and one of the most readily measurable factors) estimates were developed for the current level and near-term future levels of technology use by the four load types included in the FOT.

8.3.1   Estimation of Current and Expected Annual Growth in Technology Usage

To assess the propensity of carriers to adopt particular technology solutions, the Deployment Team surveyed motor carriers transporting HAZMAT in the second and third quarter of 2003. When returned by 153 motor carriers, the survey questionnaire produced a broad diversity of responses regarding fleet sizes, range of operations, routing variability, and general operational characteristics. The surveyed motor carriers provided the levels of fleet management technologies currently used and those to be employed in the near-term (3 years future).

The Evaluation Team recognizes that the responses to the Deployment Team survey represent approximately 0.6 percent of HAZMAT carriers considered in this analysis, a relatively thin sample on which to base market projections.

To assess possible over/under estimation within fleet size and technology bins for the Deployment Team's HAZMAT Industry Technology Analysis, the results of two other industry technology surveys were reviewed.[25] Additionally, a study of technology use by over 900 motor carriers conducted for FMCSA also was consulted.[26] These sources, while suggestive in content, enabled the validation of initial approximations of current technology usage by carriers derived through the HAZMAT Industry Technology Analysis.

8.3.2   Estimated Current Use of Technology by HAZMAT Carriers

The estimated percentage of fleets using the FOT-technologies was applied to the fleet size demographics presented in Section 2.1of this synthesis document to provide estimates of the number of technology-equipped trucks in the fleets. It is assumed that if a fleet used a particular technology, it would be used in all of the trucks associated with a particular load type. As previously noted, the more localized hauls of Bulk Fuel and LTL express or Non-Bulk-type services are assumed to use the Terrestrial Communications system rather that the Satellite Communications system.

Weighted sum averages were developed for each of the load types and technologies to derive the estimated number of trucks using the technologies. These averages were calculated by multiplying the percent distribution of fleets by size by load type by the percent of technology adoption for the fleet size bin, and then summed across a particular technology. The resultant technology percent adoption rates by load type were then multiplied by the number of trucks for each load type to estimate the maximum percent of equipped trucks within each load type. Tables outlining this information are contained in **Volume III, Section 4**.

The estimated current levels of technology deployment developed through this effort indicate that with the exception of cell phones, paging systems and two-way radio (approximately 87 percent of trucks), Satellite Communications (59 to 63 percent of trucks), and asset tracking (45 to 48 percent of trucks) technology adoption is limited among the four load types. On-Board Computers are used in approximately 12 percent of trucks and 20 percent of trucks are from fleets using Web-based shipment tracking systems (a proxy for the ESCM test system). The percentages for the other technologies are estimated to be at most 13 percent of trucks, with most below 10 percent of trucks.

It is estimated that over the next 3 years, modest annual growth is expected for the technologies: Satellite Communications (1.7 to 2.3 percent); Panic Buttons (1.3 to 1.4 percent); Vehicle Tracking (0.8 to 1.1 percent); On-Board Computers (2.4 to 2.9 percent); Automated Driver Identification (1.0 to 1.3 percent); and Remote Vehicle Disabling (1.2 to 1.4 percent). Less than 1 percent annual growth in technology adoption is expected for the remaining technologies, with especially small growth in cell phone/pager systems, as these have already approached near universal adoption.

---

[25] ATRI – GartnerG2 survey of 150 motor carriers on adoption of in-vehicle technologies, Trucking Technology Survey – 2003; ATRI industry survey of 348 motor carriers to determine levels of technology adoption in 2000 and projections to 2003, in support of the North American International Trade Corridor (NAITC) Comprehensive and Coordinated Intelligent Transportation Systems for Commercial Vehicle Operations (ITS/CVO) Plan.

[26] ATA Foundation, *Motor Carrier Technologies – Fleet Operational Impacts and Implications for Intelligent Transportation Systems/Commercial Vehicle Operations*, October 1999.

In context, the current level of technology adoption, as expressed in technology-equipped trucks, represents costs already incurred and benefits already being realized compared to the baseline (no technology) efficiency and security costs and benefits.

8.4   ESTIMATED EFFICIENCY BENEFITS AND COSTS

For the efficiency assessment, the key finding was that the participating motor carriers ascribed little operational efficiency impacts to the test technologies, with the exception of Wireless Communications with GPS tracking capabilities. The motor carriers' primary viewpoints for operational efficiency were focused on the following: the ability to communicate efficiently with drivers, to know where the vehicles are and when to manage customer requests for status and arrival times; track driver and vehicle operational performance on the road; and to effect better load planning.

8.4.1   Benefits, Costs, and ROI Summary

Using detailed quantitative operational data and qualitative perception data from the participants and archived transaction records and pricing schemas from QUALCOMM, financial performance analyses were developed for the combination of Wireless Communications with GPS asset positioning. For the industry segments, LTL-High Hazard, Bulk Chemicals, and Truckload Explosives, benefits focused on the following elements:

- Reduced telecommunications costs.

- Increased driver to dispatcher ratios.

- Reduced on-the-road downtime translated into potential load increases or trips.

- Reduced fuel consumption and engine wear.

- Reduced maintenance costs and increased revenue through decreased repair down time.

- Reduced out-of-route miles.

For Bulk Fuel and LTL-Non-Bulk operations, which as a key performance metric use driver utilization versus a calculated target (in terms of on-time performance or pounds of product moved), benefits were derived in terms of saved driver time, while holding other variables constant.

To summarize, estimated monthly benefits per truck from Section 5 of this synthesis document are:

- Bulk Fuel – $486

- LTL (Non-Bulk) – $160

- LTL-High Hazard – $196 to $820

- Bulk Chemicals – $130 to $593

- Truckload Explosives – $152 to $917

8.4.2   Cost and ROI Summary

The benefits presented in Section 6 of this synthesis document were compared to the generally, more high-end costs of the satellite- and terrestrial-based product/ service offerings to estimate benefit-cost ratios and expected payback periods. Table 8-1 presents the costs by industry segment (capital costs are amortized over 3 years). Using these costs from Table 8-1 and benefits developed in Section 5 of this synthesis document, benefit-cost

ratios and payback periods in months were calculated, with the results reported in Table 8-2. The annual costs per truck include the initial purchase of equipment and installation amortized over 3 years plus annual messaging and maintenance service fees. These are from the figures presented in Table 8-1. The type of equipment – Terrestrial- versus Satellite-based assumed for each load type is: Bulk Fuel and LTL Non-Bulk-terrestrial (T) and LTL High-Hazard, Bulk Chemicals, and Truckload Explosives – Satellite (S). The choice of terrestrial- versus Satellite-based systems is based on using the lowest cost service appropriate to the operational characteristics associated with the test scenarios. For example terrestrial is more appropriate for the shorter hauls in more developed areas with good terrestrial coverage associated with the Bulk Fuel and LTL-Non-Bulk scenarios. The longer hauls in more remote areas characteristic of the Bulk Chemical, LTL-High Hazard and Truckload Explosives operations require the coverage afforded by satellite service.

Table 8-1. Per Truck-Specific Technology Costs
(Wireless Communications with GPS Tracking Capabilities)

Item	Purchase Cost/ Truck Terrestrial / Satellite	Annual Cost/ Truck Terrestrial / Satellite
Mobile Communications with GPS Tracking Units (Hardware Costs)	$1,000 / $2,000	$336 / $672
Installation	$200	$72
Basic Monthly Service (per truck)[27]		$600
Monthly Maintenance Agreement		$180
Total Per Truck Costs	**$1,200 / $2,200**	**$1,188 / $1,524**

Table 8-2. Costs, Benefits, Benefit-Cost Ratios, and Payback Periods
by Industry Segment
(Wireless Communications with GPS Tracking Capabilities)

Segment/ Fleet Size	Annual Cost/Truck[28]	Annual Benefit/Truck	Benefit - Cost Ratio	Payback on Purchase in Months
Bulk Fuel (Terrestrial)	$1,188	$5,832	4.9:1	3
LTL-High Hazard (Satellite)	$1,524	$2,352 to $9,840	1.5:1 to 6.5:1	3 to 17
LTL Non-Bulk (Terrestrial)	$1,188	$1,920	1.6:1	13
Bulk Chemicals (Satellite)	$1,524	$1,560 to $7,116	1.0:1 to 4.7:1	5 to 34
Truckload Explosives (Satellite)	$1,524	$1,824 to $11,004	1.2:1 to 7.2:1	3 to 25

Though not all industry segments would realize significant benefit from this combination of technologies (i.e., one-truck fleets), one key parameter must be met to realize the potential

---

[27] Monthly service fees cover hourly positioning and base number of messages per unit.

[28] Costs include purchase and installation costs amortized over 3 years, plus ongoing messaging and maintenance costs.

for these systems among industry segments in which benefits could be realized – delivering financial break even in a relatively short time period of time. The payback periods estimated for the high-end units are within documented ranges for maximum time period that most motor carriers are willing to accept for return on investment.

In a survey of 100 motor carriers conducted in late 2002 by ATRI and GartnerG2, it was found that across all respondents, only 28 percent would accept a payback period between 2 and 3 years, of which only one in four would be willing to accept a payback period in excess of 3 years. The potential market penetration rate more than doubles to 59 percent if the payback period decreases to between 1 and 2 years.[29] The survey also noted that increased potential market penetration occurs more robustly with shorter payback timeframes in small- and mid-sized fleets than in larger fleets.

Smaller fleets comprise a considerable proportion of the trucking industry. These fleets also adopt technologies at a less robust rate than their larger counterparts. In part, this is due to limited need for advanced communications; tracking and decision support to manage a small fleet; limited time and capital to invest in and train on new technology solutions; limited desire to move from accepted "tried and true" ways of conducting their businesses; and lesser over time, limited low-price, high functionality product offerings. For small fleets of less than nine trucks, 91 and 60 percent of respondents would accept a maximum payback period of 6 to 12 months and 13 to 24 months, respectively, for new technology purchases. In the ROI analysis summarized above, even with considering a product on the high end of the pricing scale, the estimated payback periods would be attractive to many fleets. In the example of LTL, the 13-month payback period assumed a very conservative benefit metric; therefore, a payback period of less than 12 months is likely.

Given the breadth of product offerings, documented in the Deployment Team's Technology Compendium, basic communications and tracking capabilities can be obtained for as low as $25 to $50 per month, but without the capabilities of additional technology add-ons.

8.4.3   Industry Deployment and Potential ROI

Given the conservative range of benefit estimates and using the high-end of technology costs, potential industry benefits and costs were derived. These are presented in Table 8-3. In defining the market potential, it is recognized that there may be minimum fleet sizes in these sectors under which the usefulness of integrated communications and tracking systems may be easily reproduced with less advanced methods and technologies, such as cell phones and pagers. Therefore, it is assumed that fleets of less than 10 trucks would not migrate from basic cell phone/pager communications systems to an integrated Wireless Communications system with GPS positioning due to a lesser need for technology-enhanced fleet management in this class of carriers.

Eliminating fleets of nine trucks or less would remove 3,995, 2,262, 6,965, 1,507, and 389 trucks from the market potential for Bulk Fuel, LTL-High Hazard, LTL-Non-Bulk Service, Bulk Chemicals, and Truckload Explosives sectors, respectively. The new total "trucks by industry" segment is referred to as "New Market Potential." The analysis in Table 8-3 shows that approximately 54 percent of potential market has yet to be realized.[30]

---

[29] ATRI – GartnerG2 Trucking Technology Survey, December 2002.
[30] In estimating current levels of market penetration, the current deployment levels for the most limiting technology – Vehicle Tracking – was used.

**Table 8-3. Current Industry Deployment Levels
Versus Unrealized Industry Market Potential
(Wireless Communications with GPS Tracking Capabilities)**

Load Type	New Potential Market	Current Penetration	% Current Penetration	Unrealized Market Potential
Bulk Fuel	111,031 Trucks	51,768 Trucks	47%	59,264 Trucks
LTL-High Hazard	145,184 Trucks	70,779 Trucks	49%	74,405 Trucks
LTL-Non-Bulk	368,380 Trucks	178,926 Trucks	49%	189,454 Trucks
Bulk Chemicals	61,168 Trucks	28,963 Trucks	47%	32,204 Trucks
Truckload Explosives	8,195 Trucks	3,823 Trucks	47%	4,373 Trucks

To realize the full potential benefits *(moving from current levels of deployment to full deployment)*, it is estimated that the HAZMAT trucking industry (at the high end) would have to invest an initial $543 million and incur annual service fees of $829 million per year. If the purchase costs were amortized over 3 years, total annual costs (including monthly service fees) would be approximately $457 million. Offsetting these costs would be increase profitability, estimated to range from $943 million to $1.7 billion per year. These estimates are presented in Table 8-4.[31]

---

[31] Bulk fuel shipments include bulk shipments of: Class 3: Flammable/Combustible Liquids and Class 2, Division 2.1: Flammable Gases; LTL-High Hazard includes non-bulk shipments of: Class 2, Divisions 2.3A-2.3D: (PIH Zones-A-D, respectively), Class 4, Divisions 4.1-4.3: Flammable Solids, Spontaneously Combustible Materials, Dangerous When Wet Material and Class 6, Division 6.1: Poison Liquid-PIH Zones A & B, Poisonous Solids; LTL-Express or Non-Bulk Type Service includes non-bulk shipments of: Class 3: Flammable/Combustible Liquids; Class 7: Radioactive Materials; Class 8: Corrosive Materials; Bulk Chemicals includes bulk shipments of: Class 2, Division 2.2A: Anhydrous Ammonia; Class 5, Divisions 5.1-5.2: Oxidizers, Organic Peroxide; Class 6, Division 6.1: Poison Liquid-PIH Zones A & B, Poisonous Solids; Truckload Explosives includes bulk shipments of: Class 1, Divisions 1.1-1.6: Explosives and Blasting Agents.

**Table 8-4. Industry Efficiency Benefit and Cost Estimates/Investments Over 3 Years
for Wireless Communications with GPS Tracking Capabilities
(In Millions of Dollars)**

Load Type	Unrealized Market Potential	Technology Investment	Investment Amortized Over 3 Years	Annual Service Fees	Total Annual Costs	Total Annual Benefits
Bulk Fuel	59,264 Trucks	$71	$24	$46	$69	$346
LTL-High Hazard	74,405 Trucks	$164	$55	$57	$112	$175 to $732
LTL-Non-Bulk	189,454 Trucks	$227	$76	$146	$221	$364
Bulk Chemicals	32,204 Trucks	$71	$24	$25	$48	$50 to $229
Truckload Explosives	4,373 Trucks	$10	$3	$3	$7	$8 to $48
Totals	359,700 Trucks	$543	$181	$276	$457	$943 to $1,719

8.5   ESTIMATED SECURITY BENEFITS AND COSTS

8.5.1 Benefits-Consequence Avoidance

As presented in Section 6.3 of this synthesis document, security benefits were defined as potential reductions in the costs or consequences of truck-based HAZMAT attacks. These were derived by applying the estimated percent reductions in HAZMAT trucking vulnerabilities to the reasonable worst-case consequences of attacks using HAZMAT. The reduction vulnerabilities translate directly into the reduction in probability that a HAZMAT load will be successfully used in an attack. **It should be noted that partial deployment might not necessarily result in a directly proportional security benefit. In other words, 50 percent deployment may not yield 50 percent of achievable security benefits.** This may occur because while the technology-equipped fleet may not be attacked, a non-equipped fleet would possibly be targeted instead. The deterrent effect of the technologies, if partly deployed, could simply shift terrorist targeting from one fleet to another, with no net change in overall security. Under this assumption, then full deployment is required to realize the security benefits.

For each technology combination and load type, attack cost reductions (benefits) were calculated. For the convenience of the reader, these are reiterated in Table 8-5 and later presented in Table 8-10 as part of the security benefit-cost ratio presentation.

**Table 8-5. Estimated Security Benefits by Load Type and Technology
(In Millions of Dollars)**

Technology	Bulk Fuel	LTL	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$548	$268	$1,917	$1,409
WC + GPS Position (Baseline)	$622	$348	$2,581	$1,657
Panic Alert + (WC + GPS Position)	$995	$529	$4,058	$2,822
Driver ID + (WC + GPS Position)	$933	$537	$3,730	$2,345
Vehicle Disabling (+WC + GPS)	$970	$573	$4,278	$2,556
Cargo Seals (+WC + GPS Position)	NA	$529	NA	$2,345
Cargo Door Locks (+WC + GPS Position)	NA	$513	NA	$2,400
PSRC (+WC + GPS)	$908	$525	$3,891	$2,652
ESCM (+WC + GPS) incl. Biometric Driver ID	$946	$553	$3,730	$2,400
Panic Alert + Vehicle Disabling + (WC + GPS)	$1,207	$689	$5,098	$3,355
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$1,331	$776	$5,539	$3,547
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$1,318	$755	$5,319	$3,510
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	$755	NA	$3,469
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	$747	NA	$3,510

8.5.2   Costs

Costs are defined as the expense of purchasing and installing technology initially, plus ongoing message service (including hourly position reports) and maintenance fees.[32] The ongoing costs are assumed for 3 years, with annual discounting of 1.016 percent, per OMB requirements for discounting future cash flows.[33] The technology costs are based on the pricing tiers proposed in the Deployment Team's Concept of Operations and fielded during the FOT, adjustments to the FOT pricing following test deployment, and consultation with the Deployment Team's Technology Compendium.[34]

Table 8-6 presents the estimated per truck costs for the technologies by technology scenario and load type over 3 years. The figures in this table assume that if a carrier hauls one of the scenario load types, then all of the trucks in this fleet as reported in MCMIS are assigned to

---

[32] Potential costs not included in the analysis are vehicle downtime for installation and training time for personnel. Through discussions with motor carriers and the technology vendor, installation would likely occur during schedule downtime for preventive maintenance. Training of personnel in the use of technologies would generally fall within usual new employee training/orientation processes or within ongoing carrier training/skills enhancement activities.

[33] U.S. Office of Management and Budget – *Circular No. A-94 – Appendix C – Discount Rates for Cost Effectiveness*, Revised February 2004.

[34] Battelle, in association with QUALCOMM, ATRI, CVSA, and the Spill Center, *HAZMAT Safety and Security Field Operational Test Draft Final Report*, June 11, 2004.

the load type. The exception is where more than one HAZMAT type is indicated for a fleet, in that case, the fleet vehicles are split evenly between the load types. This assumption assures that if non-HAZMAT dedicated equipment is used in transporting HAZMAT, then the costs of realizing the technology security benefits are fully accounted for. These two sets of estimates enable the calculation of break even points for number of successful attacks and potential benefit-cost ratios for the technologies (and combinations of technologies) as a whole.

Table 8-6. Estimated Per Truck Costs by Technology Over 3 Years

Technology	Bulk Fuel	LTL[35]	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$1,822	$1,822	$1,822	$1,822
WC + GPS Position (Baseline)	$3,504	$4,204	$4,504	$4,504
Panic Alert + (WC + GPS Position)	$3,704	$4,404	$4,704	$4,704
Driver ID + (WC + GPS Position)	$3,804	$4,504	$4,804	$4,804
Vehicle Disabling (+WC + GPS)	$3,804	$4,504	$4,804	$4,804
Cargo Seals (+WC + GPS Position)	NA	$4,704	NA	$5,004
Cargo Door Locks (+WC + GPS Position)	NA	$4,704	NA	$5,004
PSRC (+WC + GPS)36	$3,554	$4,254	$4,554	$4,554
ESCM (+WC + GPS) incl. Biometric Driver ID	$4,004	$4,704	$5,004	$5,004
Panic Alert + Vehicle Disabling + (WC + GPS)	$4,004	$4,704	$5,004	$5,004
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$4,304	$5,004	$5,304	$5,304
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$4,504	$5,204	$5,504	$5,504
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	$5,504	NA	$5,804
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	$5,504	NA	$5,804

For the "Total Deployment Costs," all trucks assigned to the load type are assumed to be equipped with the technology. For the "Marginal Deployment Costs" (i.e., the costs that would have to be incurred above current and committed to deployment), it was assumed that the number of trucks to be equipped is based on the most limiting technology in the combination (the technology requiring the most number of trucks to be equipped).

For example, to reach full deployment for a technology combination of X technology requiring 9 trucks to be equipped and Y technology requiring 10 trucks to be equipped, then the methodology assumes 10 trucks to be equipped for both technologies. This is done in

---

[35] The costs for LTL are averages of LTL-High Hazard and LTL-Non-Bulk weighted by numbers of trucks in each category.

[36] The Public Sector Reporting Center (PSRC) is not a commercial service, but it is built upon the provider's basic technology and service offering. The subscription rates for fleets range from approximately $1,200 to $2,500 per fleet. The PSCR cost component is calculated as: (number of fleets by load time x Subscription rate) / number of trucks in each load type. Costs do not include public sector hardware interfaces with the Spill Center. The costs per unit represent 3 years of subscription fees.

recognition that product integration issues may require a total refit of the technologies in the combination. Table 8-7 presents these estimated numbers of trucks.

Table 8-7. Number of Trucks to be Equipped to Realize Full Deployment Potential

Technology	Bulk Fuel	LTL	Bulk Chemicals	Truckload Explosives
Total Number of Trucks by Load Type	115,026	522,793	62,675	8,287
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	22,326	105,199	12,385	1,651
WC with GPS Positioning	44,007	188,104	23,573	3,229
Mayday or Driver Panic Buttons	100,839	464,468	55,469	7,452
Automated Driver ID System	98,148	448,538	53,833	7,212
Remote Vehicle Disabling System	105,897	488,902	58,300	7,823
Electronic Cargo Seals/ Locks	111,031	513,564	61,168	8,181
Web-Based Shipment Tracking System (Proxy for Electronic Manifesting)	88,115	402,122	48,306	6,503
Public Safety Reporting Center (PSRC)[37]	115,026	522,793	62,675	8,287

Given current levels of deployment, Table 8-8 presents the "**Marginal Deployment Costs**" or the costs that would need to be incurred to move from the current deployment levels to full deployment. These **are presented to provide the reader with the levels of investment that would be required above current levels to realize full deployment**. The **Total Full Deployment Costs (all trucks)** is presented in Table 8-9, and **is used with the security benefits previously presented to derive benefit-cost ratios for the technologies.**

---

[37]This is not a commercial offering; therefore, all vehicles are considered potential market. It is assumed that the fleets are not currently enrolled in the provider's base notification system for costing purposes.

Table 8-8. Marginal Deployment Costs for Future Investment Above Current Levels Required to Reach Full Deployment) By Technology Combination and Load Type Including 3 Years of Service Fees (In Millions of Dollars)

Technology	Bulk Fuel	LTL[38]	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$41	$192	$23	$3
WC + GPS Position (Baseline)	$154	$791	$106	$15
Panic Alert + (WC + GPS Position)	$373	$2,045	$261	$35
Driver ID + (WC + GPS Position)	$373	$2,020	$259	$35
Vehicle Disabling (+WC + GPS)	$403	$2,202	$280	$38
Cargo Seals (+WC + GPS Position)	NA	$2,416	NA	$41
Cargo Door Locks (+WC + GPS Position)	NA	$2,416	NA	$41
PSRC (+WC + GPS)	$409	$2,224	$285	$747
ESCM (+WC + GPS) incl. Biometric Driver ID	$393	$2,110	$269	$36
Panic Alert + Vehicle Disabling + (WC + GPS)	$424	$2,300	$292	$39
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$456	$2,446	$309	$41
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$477	$2,544	$321	$43
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	$2,826	NA	$47
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	$2,826	NA	$47

---

[38] The costs for LTL are averages of LTL-High Hazard and LTL-Non-Bulk weighted by numbers of trucks in each category.

Table 8-9. Total Full Deployment Costs By Technology Combination and Load Type Including 3 Years of Service Fees (In Millions of Dollars)

Technology	Bulk Fuel	LTL	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$210	$953	$114	$15
WC + GPS Position (Baseline)	$403	$2,198	$282	$37
Panic Alert + (WC + GPS Position)	$426	$2,302	$295	$39
Driver ID + (WC + GPS Position)	$438	$2,354	$301	$40
Vehicle Disabling (+WC + GPS)	$438	$2,354	$301	$40
Cargo Seals (+WC + GPS Position)	NA	$2,459	NA	$41
Cargo Door Locks (+WC + GPS Position)	NA	$2,459	NA	$41
PSRC (+WC + GPS)	$409	$2,224	$285	$38
ESCM (+WC + GPS) incl. Biometric Driver ID	$461	$2,459	$314	$41
Panic Alert + Vehicle Disabling + (WC + GPS)	$461	$2,459	$314	$41
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$495	$2,616	$332	$44
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$518	$2,720	$345	$46
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	$2,720	NA	$48
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	$2,877	NA	$48

8.5.3 Benefits Versus Costs

The effort estimated the potential benefit-cost ratios for the technology countermeasures. A key variable for this calculation of benefit-cost ratios is the estimated overall reductions in vulnerabilities developed through the Delphi process, discussed in Section 6 of this synthesis document, and applied to the potential consequences of terrorist attacks using HAZMAT.

Using the **Total Deployment Costs** from Table 8-8 and benefits from Table 8-5, benefit-cost ratios were developed for the technologies. These security benefit cost-ratios are presented in Table 8-10. *These figures are not additive across load types.*

As displayed in Table 8-10, all technology scenarios across three of the four load types demonstrate potential security benefit-cost ratios greater than 1 using assumed high costs and conservatively estimated benefits. The obvious exceptions are the LTL scenarios in which the potential consequence and attractiveness of the LTL loads for use as a weapon of mass effect is relatively low and the number of trucks that would require being equipped is relatively high.

Table 8-10. Estimated Total Security Benefits and Costs Over 3 Years by Technology and Load Type (In Millions of Dollars)

Load Type > Technology	Bulk Fuel			LTL[39]			Bulk Chemicals			Truckload Explosives		
	Cost	Benefit	Benefit-Cost Ratio	Cost	Benefit	Benefit-Cost Ratio	Cost	Benefit	Benefit-Cost Ratio	Cost	Benefit	Benefit-Cost Ratio
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$210	$548	2.6	$953	$268	0.3	$114	$1,917	16.8	$15	$1,409	93.9
WC + GPS Position	$403	$622	1.5	$2,198	$348	0.2	$282	$2,581	9.2	$37	$1,657	44.8
Panic Alert + (WC + GPS Position)	$426	$995	2.3	$2,302	$529	0.2	$295	$4,058	13.8	$39	$2,822	72.4
Driver ID + (WC + GPS Position)	$438	$933	2.1	$2,354	$537	0.2	$301	$3,730	12.4	$40	$2,345	58.6
Vehicle Disabling + (WC + GPS)	$438	$970	2.2	$2,354	$573	0.2	$301	$4,278	14.2	$40	$2,556	63.9
Cargo Seals (+WC + GPS Position)	NA	NA	NA	$2,459	$529	0.2	NA	NA	NA	$41	$2,345	57.2
Cargo Door Locks + (WC + GPS Position)	NA	NA	NA	$2,459	$513	0.2	NA	NA	NA	$41	$2,400	58.5
PSRC (+WC + GPS)	$409	$908	2.2	$2,224	$525	0.2	$285	$3,891	13.7	$38	$2,652	69.8
ESCM (+WC + GPS) incl. Biometric Driver ID	$461	$946	2.1	$2,459	$553	0.2	$314	$3,730	11.9	$41	$2,400	58.5
Panic Alert + Vehicle Disabling + (WC + GPS)	$461	$1,207	2.6	$2,459	$689	0.3	$314	$5,098	16.2	$41	$3,355	81.8
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$495	$1,331	2.7	$2,616	$776	0.3	$332	$5,539	16.7	$44	$3,547	80.6
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$518	$1,318	2.5	$2,720	$755	0.3	$345	$5,319	15.4	$46	$3,510	76.3
Panic Alert + Driv. ID + Veh. Disabling + Cargo Seals (WC + GPS)	NA	NA	NA	$2,720	$755	0.3	NA	NA	NA	$48	$3,469	72.3
Panic Alert+Driv. ID+Veh. Disabling+Cargo Door Locks (WC+GPS)	NA	NA	NA	$2,877	$747	0.3	NA	NA	NA	$48	$3,510	73.1

---

39 The costs for LTL are averages of LTL-High Hazard and LTL-Non-Bulk Service costs weighted by numbers of trucks in each category.

8.5.4   Breakeven Points

As discussed in Section 6.3 of this synthesis document, the security benefits were derived under the assumption that threat is held constant at a 100 percent chance that an attempt will be made over the next 3 years on/using a HAZMAT load for a terrorist attack. Realizing that threat can be unpredictable and vary over time, breakeven numbers of successful attacks that would need to be reduced via the technologies to equal the costs of deploying the technologies is proffered. These breakeven values were calculated using the following formula:

Breakeven Number of Attacks =

(Total Deployment Cost for the Technology / Consequence per Attack)

For example, for Bulk Fuel, the breakeven number of successful attacks avoided for the technology wireless communications with GPS positioning is calculated as follows:

Breakeven Number of Attacks =

($403 Million Deployment Costs / $3,746 Million Consequence)

= 0.11 Successful Attacks to be Prevented for Breakeven

The above example demonstrates that security benefits would equal technology costs if **0.11** attacks were prevented over 3 years by the technology. Table 8-11 presents the estimated breakeven number of successful attacks. The breakeven probabilities are presented as a decision tool – if one believes that the probability of an attack (threat) is greater than the breakeven for a technology combination for a load type, so then to society, the investment in the technology combination can be considered sound.

For context, the highest breakeven numbers for each load type were compared to prognostications made by the Delphi Panel as to the number of attack attempts on/using truck-based HAZMAT shipments and the proportion of those attempts that are likely to be successful within the next 3 years. The Delphi Panel, at the low end, indicated the number of successful attacks as being likely exceed the breakeven attack numbers for all load types, except LTL-High Hazard loads. In summary, for all load types, except LTL-High Hazard, the Panelists feel there is at least a 5 times greater probability of successful attack than is required for equating security benefits with deployment costs.

**Table 8-11. Estimated Number of Successful Attacks to Be Prevented
to Realize Breakeven with Deployments Costs**

Technology	Bulk Fuel	LTL	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	0.056	0.449	0.007	0.001
WC + GPS Position (Baseline)	0.108	1.036	0.017	0.003
Panic Alert + (WC + GPS Position)	0.114	1.085	0.018	0.003
Driver ID + (WC + GPS Position)	0.117	1.109	0.018	0.003
Vehicle Disabling (+WC + GPS)	0.117	1.109	0.018	0.003
Cargo Seals (+WC + GPS Position)	NA	1.159	NA	0.003
Cargo Door Locks (+WC + GPS Position)	NA	1.159	NA	0.003
PSRC (+WC + GPS)40	0.109	1.048	0.017	0.003
ESCM (+WC + GPS) incl. Biometric Driver ID	0.123	1.159	0.019	0.003
Panic Alert + Vehicle Disabling + (WC + GPS)	0.123	1.159	0.019	0.003
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	0.132	1.233	0.020	0.003
Panic Alert + Driver ID + ESCM (WC + GPS Position)	0.138	1.282	0.021	0.003
Panic Alert + Driver ID + Vehicle Disabling + Cargo Seals (WC + GPS Position)	NA	1.282	NA	0.004
Panic Alert + Driver ID + Vehicle Disabling + Cargo Door Locks (WC + GPS Position)	NA	1.356	NA	0.004

---

[40] The Public Sector Reporting Center (PSRC) is not a commercial service, but it is built upon the provider's basic technology and service offering. The subscription rates for fleets range from approximately $1,200 to $2,500 per fleet. The PSCR cost component is calculated as: (number of fleets by load time x Subscription rate) / number of trucks in each load type. Costs do not include public sector hardware interfaces with the Spill Center. The costs per unit represent 3 years of subscription fees.

8.6   CONSOLIDATED BENEFITS AND COSTS

The findings of the safety, security and efficiency benefit assessments and the industry deployment-benefit-cost analyses were stand-alone analyses examining the economic feasibility of the technologies within each context. To understand the overall economic impacts, the results of the three assessments are consolidated in this section and illustrated in Tables 8-12 through 8-15.

It should be noted that:

- The efficiency benefits presented are the low estimates developed in Section 5.

- Safety benefits derived through this evaluation were primarily qualitative in nature, and those benefits that were quantified are allocated based on the percent of crash involvement by load type. Also, the potential safety benefit is assigned to all technology combinations using the core combination of Wireless Communications with GPS tracking.

- Security benefits are derived as reductions in HAZMAT shipping vulnerabilities (i.e., the probability that a shipment would successfully be used for an attack) and therefore, reduced potential consequences of terrorist activity.

**Table 8-12. Consolidated Annual Benefits and Costs
by Technology for Bulk Fuel
(In Millions of Dollars)**

Technology	Bulk Fuel					
	Cost	Security Benefit	Efficiency Benefit	Safety Benefit	Total Benefits	Benefit-Cost Ratio
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$210	$548	$2,012	$4.2	$2,565	12.2
WC + GPS Position	$403	$622	$2,012	$4.2	$2,639	6.5
Panic Alert + (WC + GPS Position)	$426	$995	$2,012	$4.2	$3,012	7.1
Driver ID + (WC + GPS Position)	$438	$933	$2,012	$4.2	$2,950	6.7
Vehicle Disabling + (WC + GPS)	$438	$970	$2,012	$4.2	$2,987	6.8
Cargo Seals (+WC + GPS Position)	NA	NA	NA	NA	NA	NA
Cargo Door Locks + (WC + GPS Position)	NA	NA	NA	NA	NA	NA
PSRC (+WC + GPS)	$409	$908	$2,012	$4.2	$2,925	7.2
ESCM (+WC + GPS) incl. Biometric Driver ID	$461	$946	$2,012	$4.2	$2,963	6.4
Panic Alert + Vehicle Disabling + (WC + GPS)	$461	$1,207	$2,012	$4.2	$3,224	7.0
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$495	$1,331	$2,012	$4.2	$3,348	6.8
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$518	$1,318	$2,012	$4.2	$3,335	6.4
Panic Alert + Driv. ID + Veh. Disabling + Cargo Seals (WC + GPS)	NA	NA	NA	NA	NA	NA
Panic Alert+Driv. ID+Veh. Disabling+Cargo Door Locks (WC+GPS)	NA	NA	NA	NA	NA	NA

**Table 8-13. Consolidated Annual Benefits and Costs
by Technology for LTL
(In Millions of Dollars)**

Technology	LTL					
	Cost	Security Benefit	Efficiency Benefit	Safety Benefit	Total Benefits	Benefit-Cost Ratio
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$953	$268	$3,202	$0.2	$3,470	3.6
WC + GPS Position	$2,198	$348	$3,202	$0.2	$3,551	1.6
Panic Alert + (WC + GPS Position)	$2,302	$529	$3,202	$0.2	$3,732	1.6
Driver ID + (WC + GPS Position)	$2,354	$537	$3,202	$0.2	$3,740	1.6
Vehicle Disabling + (WC + GPS)	$2,354	$573	$3,202	$0.2	$3,776	1.6
Cargo Seals (+WC + GPS Position)	$2,459	$529	$3,202	$0.2	$3,732	1.5
Cargo Door Locks + (WC + GPS Position)	$2,459	$513	$3,202	$0.2	$3,716	1.5
PSRC (+WC + GPS)	$2,224	$525	$3,202	$0.2	$3,728	1.7
ESCM (+WC + GPS) incl. Biometric Driver ID	$2,459	$553	$3,202	$0.2	$3,756	1.5
Panic Alert + Vehicle Disabling + (WC + GPS)	$2,459	$689	$3,202	$0.2	$3,892	1.6
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$2,616	$776	$3,202	$0.2	$3,979	1.5
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$2,720	$755	$3,202	$0.2	$3,958	1.5
Panic Alert + Driv. ID + Veh. Disabling + Cargo Seals (WC + GPS)	$2,720	$755	$3,202	$0.2	$3,958	1.5
Panic Alert+Driv. ID+Veh. Disabling+Cargo Door Locks (WC+GPS)	$2,877	$747	$3,202	$0.2	$3,950	1.4

**Table 8-14. Consolidated Annual Benefits and Costs
by Technology for Bulk Chemicals
(In Millions of Dollars)**

Technology	Bulk Chemicals					
	Cost	Security Benefit	Efficiency Benefit	Safety Benefit	Total Benefits	Benefit-Cost Ratio
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$114	$1,917	$293	$0.4	$2,211	19.4
WC + GPS Position	$282	$2,581	$293	$0.4	$2,875	10.2
Panic Alert + (WC + GPS Position)	$295	$4,058	$293	$0.4	$4,352	14.8
Driver ID + (WC + GPS Position)	$301	$3,730	$293	$0.4	$4,024	13.4
Vehicle Disabling + (WC + GPS)	$301	$4,278	$293	$0.4	$4,572	15.2
Cargo Seals (+WC + GPS Position)	NA	NA	NA	NA	NA	NA
Cargo Door Locks + (WC + GPS Position)	NA	NA	NA	NA	NA	NA
PSRC (+WC + GPS)	$285	$3,891	$293	$0.4	$4,185	14.7
ESCM (+WC + GPS) incl. Biometric Driver ID	$314	$3,730	$293	$0.4	$4,024	12.8
Panic Alert + Vehicle Disabling + (WC + GPS)	$314	$5,098	$293	$0.4	$5,392	17.2
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$332	$5,539	$293	$0.4	$5,833	17.6
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$345	$5,319	$293	$0.4	$5,613	16.3
Panic Alert + Driv. ID + Veh. Disabling + Cargo Seals (WC + GPS)	NA	NA	NA	NA	NA	NA
Panic Alert+Driv. ID+Veh. Disabling+Cargo Door Locks (WC+GPS)	NA	NA	NA	NA	NA	NA

**Table 8-15. Consolidated Annual Benefits and Costs
by Technology for Truckload Explosives
(In Millions of Dollars)**

Technology	Truckload Explosives					
	Cost	Security Benefit	Efficiency Benefit	Safety Benefit	Total Benefits	Benefit-Cost Ratio
Wireless Communications (WC) – Cellular Phones, Pagers, Two-Way Radios	$15	$1,409	$45	$0.20	$1,454	96.9
WC + GPS Position	$37	$1,657	$45	$0.20	$1,702	46.0
Panic Alert + (WC + GPS Position)	$39	$2,822	$45	$0.20	$2,867	73.5
Driver ID + (WC + GPS Position)	$40	$2,345	$45	$0.20	$2,390	59.8
Vehicle Disabling + (WC + GPS)	$40	$2,556	$45	$0.20	$2,601	65.0
Cargo Seals + (WC + GPS Position)	$41	$2,345	$45	$0.20	$2,390	58.3
Cargo Door Locks + (WC + GPS Position)	$41	$2,400	$45	$0.20	$2,445	59.6
PSRC + (WC + GPS)	$38	$2,652	$45	$0.20	$2,697	71.0
ESCM + (WC + GPS) incl. Biometric Driver ID	$41	$2,400	$45	$0.20	$2,445	59.6
Panic Alert + Vehicle Disabling + (WC + GPS)	$41	$3,355	$45	$0.20	$3,400	82.9
Panic Alert + Driver ID + Vehicle Disabling (WC + GPS Position)	$44	$3,547	$45	$0.20	$3,592	81.6
Panic Alert + Driver ID + ESCM (WC + GPS Position)	$45	$3,510	$45	$0.20	$3,555	77.3
Panic Alert + Driv. ID + Veh. Disabling + Cargo Seals (WC + GPS)	$48	$3,469	$45	$0.20	$3,514	73.2
Panic Alert+Driv. ID+Veh. Disabling + Cargo Door Locks (WC+GPS)	$48	$3,510	$45	$0.20	$3,555	74.1

8.7   DISTRIBUTION OF BENEFITS AMONG PRIVATE AND PUBLIC STAKEHOLDERS

Within the framework of this evaluation, efficiency benefits are assumed to accrue to private sector motor carriers. Security and safety benefits are assumed to accrue to the general public. The costs of deploying the technologies, if market driven would be assumed by motor carriers, but if sufficient compelling societal benefits exist, then methods of cost sharing may be considered as a policy option.

As demonstrated from the analyses presented in this synthesis document, efficiency benefits outweigh the costs of deployment in all load types. This is true except for the majority of technology combinations above and beyond Wireless Communications with GPS positioning for Bulk Chemicals, and for the four technology combinations above and beyond Wireless Communications with GPS positioning for Truckload Explosives, which are at the low end of the range of potential efficiency benefits. Returns on investment for the technology combinations above and beyond Wireless Communications and GPS positioning may be marginally above the costs of deployment at the low end of benefit estimates, and therefore, may not of themselves drive adoption by motor carriers.

Security benefits are demonstrated to far outweigh deployment costs for all load types except the LTL sector, in which the types of materials carried and their quantities equate to relatively low potential consequences and the numbers of trucks to be equipped are relatively high.

Safety benefits of the technologies as calculated are relatively small in comparison the efficiency and security benefits. This is in part due to the functional nature of the technology systems themselves not being designed with a focused safety application. Overall though, the capabilities of many of the technologies do enable enhanced fleet and incident management capabilities, which can potentially translate into avoided crashes and improved response time and coordination in the event of a crash.

Table 8-16 presents the percentage of benefits realized by the private sector for each load type.

Table 8-16. Percentage of Benefits Realized by the Private Sector

Load Type	Percentage of Benefits
Bulk Fuel	60% to 72%
LTL	81% to 92%
Bulk Chemicals	5% to 13%
Truckload Explosives	1% to 3%

Figures 8-1 through 8-4 illustrate the distribution of the private and societal benefits relative to deployment costs.

Figure 8-1. Deployment Costs and Benefits by Stakeholder Type for Bulk Fuel Loads (For 3 Years – In Millions of Dollars)

Figure 8-2. Deployment Costs and Benefits by Stakeholder Type for LTL High-Hazard Loads (For 3 Years – In Millions of Dollars)
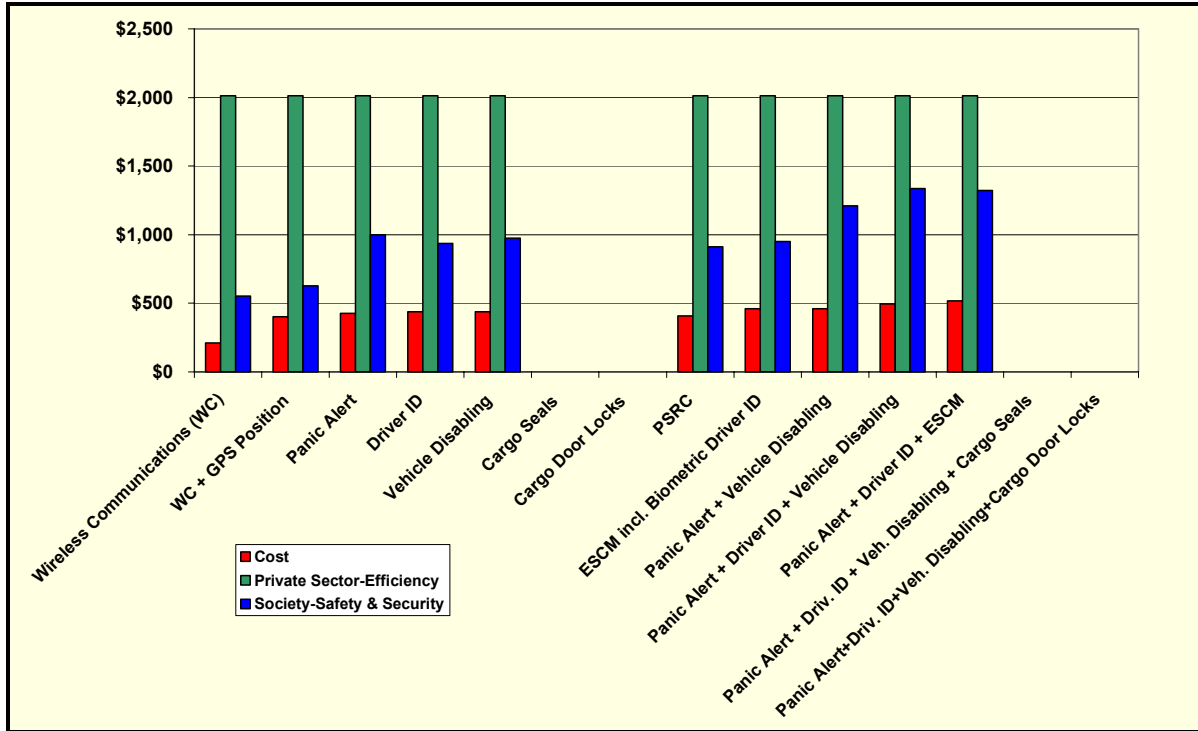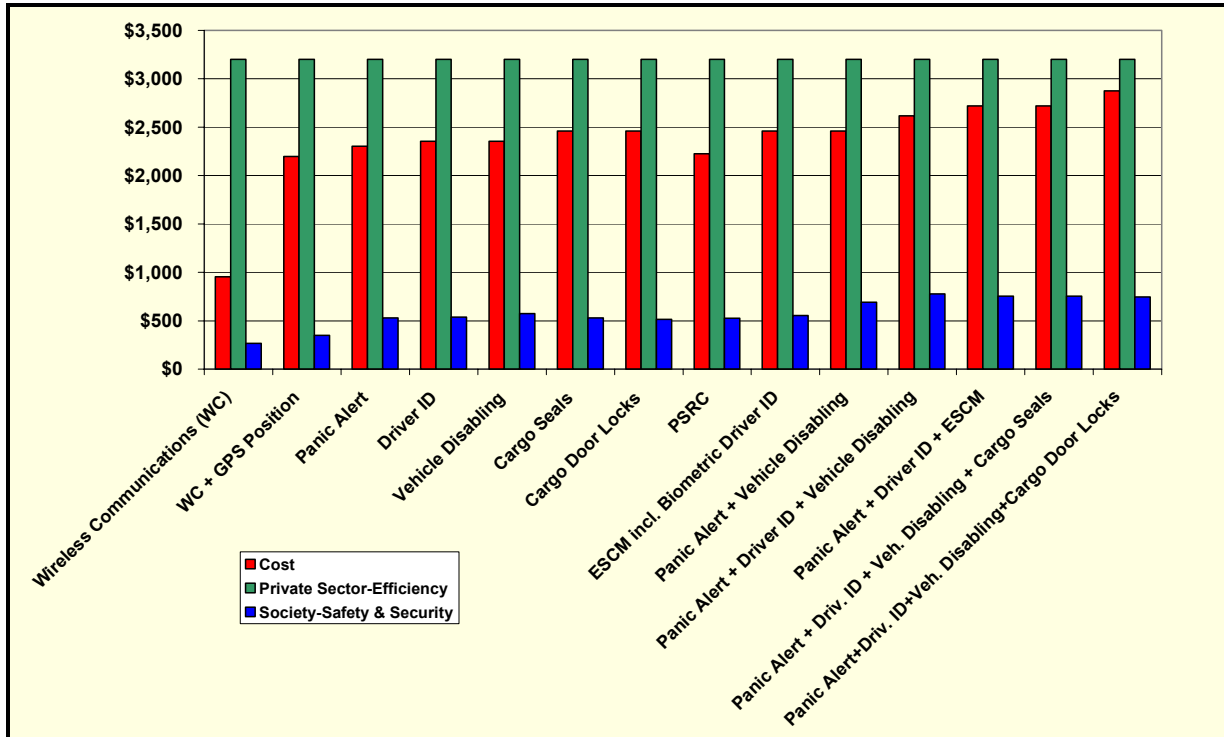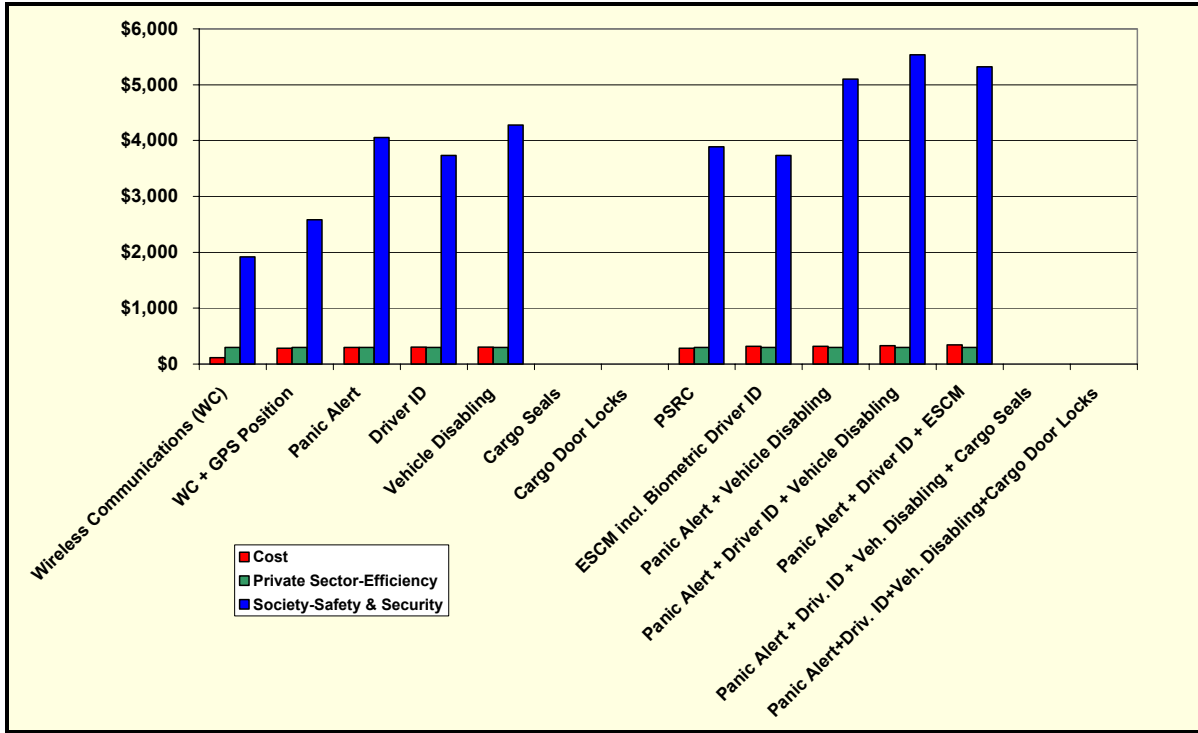
**Figure 8-3. Deployment Costs and Benefits by Stakeholder Type
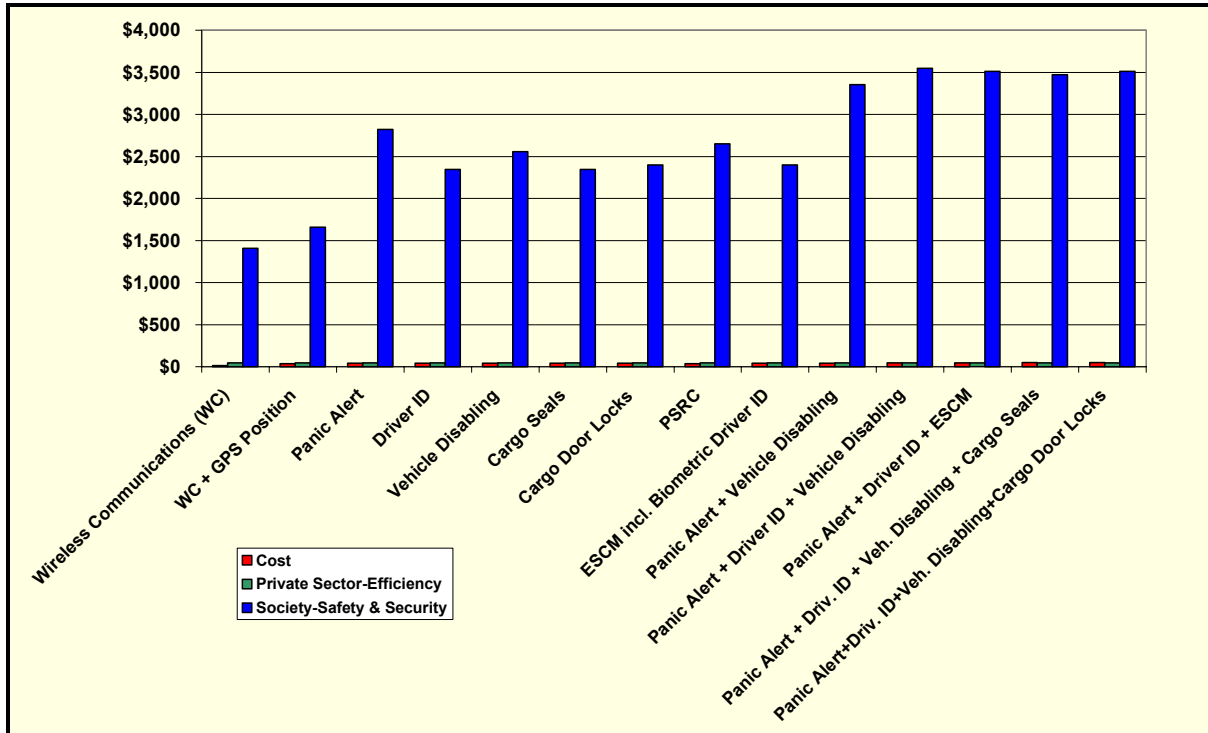for Bulk Chemical Loads (For 3 Years – In Millions of Dollars)**

**Figure 8-4. Deployment Costs and Benefits by Stakeholder Type for Truckload
Explosives Loads (For 3 Years – In Millions of Dollars)**

8.8   FINDINGS

The efficiency and security benefit-cost and market potential analyses presented in this synthesis document represent the next level of integration of the detailed Efficiency and Security Assessments detailed in **Volume III, Sections 2 and 3**, which provided methodology and analyses of operational enhancements and HAZMAT risk assessment. This synthesis document presented the universe of HAZMAT carriers and trucks that represent the potential market for security- and efficiency-enhancing technologies for four primary HAZMAT shipment types. It also detailed the levels of investment required to reach full deployment market potential and the levels of expected benefit.

Following are the findings and conclusions derived from the analyses:

- **HAZMAT Fleets:** The analysis of HAZMAT trucking companies derived from the FMCSA-managed MCMIS database shows:

  - Within the four load types, approximately 27,000 motor carriers are represented, operating 709 thousand trucks.

  - Across the four load types, approximately one-quarter to over one-third of the carriers is a one-truck operation.

  - Between 57 and 64 percent of the fleets operate 5 or fewer trucks, and between 68 and 77 percent of fleets operate fewer than 10 trucks.

- **Current Technology Usage:** Based on the FOT Industry Survey conducted by the Deployment Team and referenced against three other recent industry technology adoption survey, the results indicate:

  - Across load types, there is strong consistency in the level of use across technology types.

  - The most used technology among the fleets is cell phones consistent across load types at 87 percent.

  - The second most widely used technologies among the fleets are Satellite Communications, most often with GPS vehicle tracking, 59 to 63 percent for Satellite Communications, and 45 to 48 percent for GPS vehicle tracking.

  - On-Board Computers are used in approximately 12 percent of trucks and 20 percent of trucks are from fleets using Web-based shipment tracking systems (a proxy for the ESCM test system). The percentages for the other technologies are estimated to be at most 13 percent of trucks, with most below 10 percent of trucks.

  - As fleet size increases, the use of cell phones decreases and oppositely, the use of Satellite Communications and GPS tracking increases. This is partly due to the need for more integrated data collection and management capabilities to effectively manage larger fleets.

- **Market Potential:** Based on the MCMIS data, the following truck counts represent the universe of trucks in considering market potential:

  - By load type, the distribution of trucks is: 115,026; 52,2793; 62,675; and 8,287 trucks for the Bulk Fuel; LTL-High Hazard; Bulk Chemicals; and Truckload Explosives load types, respectively.

  - The technology suites tested in the FOT nearly all relied on the Wireless Communications with GPS positioning backbone. In terms of ROI, Wireless Communications with GPS positioning were the only technologies that demonstrated quantifiable operational benefits for the test participant's fleets. Therefore, ROI-driven

market penetration is measured based on adoption of the communications and tracking technology capabilities.[41]

– It is assumed that fleets of 1 to 9 trucks would not migrate from basic cell phone/pager two-way radio communications systems to an integrated Wireless Communications system with GPS positioning due to a lesser need for technology-enhanced fleet management in this class of carriers and the overwhelming proportion (63 percent) of these very small fleets operate within 100 miles of their base terminal, requiring limited need for tracking capabilities.

– Elimination of these very small fleets from the potential market for Wireless Communications with GPS positioning removes approximately 13,000 trucks or approximately 2 percent of the market from consideration.

– Current use of technology put the estimated penetration into the market at 47 to 49 percent of total for the combination of wireless communications with GPS tracking.

– It is estimated that for technology costs over 3 years (including costs already incurred) for full deployment range from a low of $1.3 billion (for Wireless Communications only, resulting in an average of 14 percent in potential reduction in costs of terrorist attacks) to $3.6 billion (for multiple technology combinations using Wireless Communications with GPS tracking as the enabling core technologies, resulting in an average of 36 percent in potential reduction in costs of terrorist attacks). Of these total deployment costs, approximately 20 percent (for Wireless Communications only) to 94 percent (for multiple technology combinations using Wireless Communications with GPS tracking as the enabling core technologies) represent costs associated with technology units deployed above current use levels.

• **Operational Return on Investment:** The Efficiency Assessment detailed in **Volume III, Section 2**, derived significant (conservative) benefits in relationship to (upper tier) costs for motor carriers using **Wireless Communications with GPS positioning capabilities**. These findings are summarized as follows:

– Benefits through enhanced operations are estimated at: $486; $196 to 820; $160; $130 to 593; and $152 to 941per truck per month for Bulk Fuel, LTL-High Hazard, LTL-Non-Bulk, Bulk Chemicals, and Truckload Explosives loads, respectively.

– Estimated monthly costs for the technologies (including 3-year amortization of initial purchase and installation costs and monthly messaging, positioning and maintenance fees) were from $99 to $127 per truck per month, resulting in attractive benefit cost ratios across all four load types.

– Time period for payback on investment was 3 to 13 months for all load types, assuming the upper range of benefits and 3 to 34 months assuming a low range of benefits.

– To realize the full potential benefits, it is estimated that the HAZMAT trucking industry (at the high end) would have to invest an initial $543 million and incur annual service fees of $276 million per year. If the purchase costs were amortized over 3 years, total annual costs (including monthly service fees) would be $450 million. Offsetting these costs would be increase profitability, estimated to range from $0.9 to 1.7 billion per year.

– Even with attractive ROI and low payback periods, capital constraints, institutional inertia (comfort with doing business in fixed ways), and myriad low- cost communications options are likely to make penetration of this market a long-term enterprise, especially in the smaller fleet categories.

---

[41]It is also assumed that wireless communications without the GPS tracking capability provides carriers ROI at the level estimated for wireless communications with GPS tracking.

- **Security Benefits and Costs:** The Security Assessment, detailed in **Volume III, Section 3**, was guided by the expert inputs of a steering committee and a Delphi Panel. Using a structured risk assessment framework, the results of the FOT and the experts' opinions were processed into measures of relative effectiveness of technologies to address load-specific vulnerabilities, and ultimately to reduce potential consequences of HAZMAT-based terrorist attacks. These findings include:

  – The combinations of technologies/suites tested within the FOT do have the ability to reduce the potential consequences by reducing inherent shipment vulnerabilities.

  – The most efficacious combinations of technology averaged across all four load types are estimated to address 36 percent of potential costs of terrorist attacks.

  – By load type, the reductions in of potential costs of terrorist attacks enabled by the technologies range from: 15 to 36 percent; 13 to 37 percent; 12 to 34 percent; and 11 to 26 percent for Bulk Fuel; LTL High Hazard; Bulk Chemical; and Truckload Explosives loads, respectively. In terms of human costs, the most effective technology combinations can save up to 260, 80, 1,230, and 425 casualties over 3 years for Bulk Fuel, LTL High Hazard, Bulk Chemical, and Truckload Explosives loads, respectively.[42]

  – Security benefit cost ratios are favorable for all load types, except LTL, in which the potential consequence and attractiveness of the LTL loads for use as a weapon of mass effect is relatively low and the number of trucks that would require being equipped is relatively high.

  – Costs for the Public Sector Reporting Center (PSRC) do not include stateside equipment purchase, integration and training. These costs need to be closely examined based on ultimate architecture and future plans for upgrading enforcement legacy systems.

- **Safety Benefits and Costs:** The Safety Assessment, detailed in **Volume III, Section 2,** provides quantitative and qualitative descriptions of potential safety benefits focusing on enhanced driver monitoring capabilities, reduced exposure to crashes and enhanced HAZMAT incident response. These findings include:

  – Qualitative opinion indicates that the technical capabilities of the test technologies, coupled with best practices in motor carrier driver/safety management and public sector incident response, show promise for enhancing the safety of truck-based HAZMAT shipments.

  – The technical performance of the technologies within the framework of the FOT demonstrated enhanced ability to monitor drivers and vehicles and provide notification of emergencies with location and load characteristics in a more timely manner and potentially detailed manner than traditional methods (thus potentially enhancing emergency response).

  – Through the use of proxies, potential benefits in terms of crash avoidance due to fewer miles driven and thus, reduced exposure, were estimated to be $5 million annually. No monetized benefit estimates were developed for enhanced emergency response.

- Combined Safety, Security and Operational Benefits and Costs: The combined benefit-cost findings are:

  – The driving safety and security technology (Wireless Communications with position tracking)[43] is also the driving operational technology. It has been estimated that the

---

[42] Reduced casualties were estimated by multiplying the reasonable worst-case consequence casualties from Table 6-5 by the overall technology-enabled vulnerability reductions.

[43] Though not specifically tested in this FOT, wireless communications without GPS positioning capabilities is assumed to provide all of the operational and security benefits of wireless communications with GPS.

investment in this enabling technology has the operational benefits strong enough to recoup investment and show a positive ROI in a relatively short period of time.

– Though the surplus ROI from the core enabling technology may provide the funding for additional technologies, this is not a given. Therefore, governmental or market intervention may be needed to realize full deployment of the additional security technologies.

– Under full deployment, the combined benefit-cost ratios, across all load types and technology combinations, range from 1.3:1 to 96.9:1.

– The percentage of benefits realized by the private sector for each load type is: Bulk Fuel – 60 to 72 percent of benefits; LTL – 81 to 92 percent of benefits; Bulk Chemicals – 5 to 13 percent of benefits; Truckload Explosives – 1 to 3 percent of benefits. The low percentages attributable to the private sector in the cases of Bulk Chemical and Truckload Explosives are attributable to the fact that the potential magnitude of a terrorist event using these materials is so high; the benefits due to vulnerability reduction are extremely high relative to benefits of improved efficiency.

9. PUBLIC SECTOR FOT EVALUATION

9.1   PUBLIC SECTOR FOT OVERVIEW

The Public Sector add-on FOT tested a model for enhanced information gathering, processing, and dispersal to law enforcement and emergency response agencies. This test was conducted under the auspices of the FMCSA-led HAZMAT Safety and Security FOT.

The Public Sector testing examined the potential improvements in public sector response capabilities utilizing a Public Sector Reporting Center (PSRC) as the information collection and dissemination point. The PSRC coordinated information gathered from technologies that are in various stages of development to create centralized information processing and command and control capabilities. The Public Sector testing identified quantitative and qualitative results and metrics concerning the testing of first response technologies and the PSRC concept. This overall system seems to be responsive to the following three public sector Functional Requirements developed by USDOT for the broader HAZMAT FOT:

- **Requirement 2.2:** HAZMAT driver identification and verification by roadside safety enforcement officers **was improved by at least 28 minutes**.

- **Requirement 2.4:** HAZMAT cargo route adherence by the dispatcher and roadside safety enforcement officers, as required, based on the quantity and type of HM being transported **was improved by at least 3 hours**.

- **Requirement 2.11:** Real-time emergency alert message notification by the dispatcher to local and state law enforcement officials and emergency responders **was improved by at least 18 minutes**.

The on-site Public Sector testing was augmented for this evaluation effort by data collected from technology testing from technology exercises and "staged event" testing from the full HAZMAT Safety and Security FOT (see Sections 4.2 and 4.3 of this synthesis document).

This add-on FOT to the HAZMAT Safety and Security FOT demonstrated a standardized approach to the data collection and dissemination requirements. This standardized approach seems to be efficient for the ultimate users (fire, police, emergency services, law enforcement and security agencies) of HAZMAT safety and security messages for prevention and response. The FOT demonstration for this technology solution for law enforcement and the emergency response community interfaced with the "carrier-side" technology systems. This FOT addressed some of the public sector hazardous materials safety and security needs.

Key organizations deploying the Public Sector component of this FOT included: Battelle; CVSA; QUALCOMM; and the Spill Center.

9.2   PUBLIC SECTOR REPORTING CENTER

The Public Sector FOT leveraged the following technologies that were also deployed in the larger HAZMAT Safety and Security FOT:

- Satellite Communications
- Global Login
- Biometric Global Login
- Electronic Supply Chain Manifest

- Geofencing

- Panic Buttons (In-dash and Wireless)

The public sector architecture was comprised of a Public Sector Reporting Center; Data Silo relational database; Smart Agents providing exception decision rules; and a number of information dissemination technologies.

The PSRC was designed with capabilities for data acquisition, fusion, and distribution of HAZMAT shipment information to public sector enforcement and response agencies. The PSRC integrated Wireless voice/data Communications and Satellite-tracking technology with automatic routing of alert notifications to authorities and online access to highly specialized data. The results provided real-time monitoring of HAZMAT shipment information; increased load security; and enhanced law enforcement actions and incident response in the selected test areas.

PSRC allowed end-users a Web-based application to create and manage rules that specify what conditions would trigger the alert and send a notification message. The PSRC managed user contact information including e-mail, voice text messaging on cell phones, fax, and pager numbers. The PSRC was designed to provide enhanced user functionality via:

- Viewing recent alert notification messages and near real-time vehicle data.

- Sending manual alert notifications based on driver ID, route adherence, and emergency alerts.

- Identifying response inventory and deploying response resources remotely.

Figure 9-1 (on the following page) displays the complete system architecture for the Public Sector FOT.

9.3   PUBLIC SECTOR FOT EVALUATION TESTING

The HAZMAT Safety and Security Public Sector FOT is a logical extension of the "carrier-side" evaluation. This evaluation further expanded and examined the technology and system benefits to the unique requirements of relevant local, state, and national response and enforcement agencies that deal with hazardous materials. The Evaluation Team focused on law enforcement and emergency management response metrics and user perceptions regarding deployment of the Public Sector FOT technologies and systems designed to improve detection and response to prohibited or dangerous activities involving HAZMAT shipments.

The Evaluation Team used the following two primary evaluation methods – public sector interviews and field testing – developed through bilateral discussions between SAIC and Battelle held at the request of FMCSA. These methods were be used to assess deployment technologies and systems ability to improve response time and provide more accurate, detailed information to law enforcement and incident response agencies.

9.3.1   Public Sector Interviews

Through interviews with public sector participants in the FOT, the Evaluation Team collected qualitative information concerning the quality and timeliness of information provided by the test technologies and the PSRC. Additionally, the effort collected user perceptions of effectiveness, appropriateness to the enforcement operational environment, and policy options for system enhancements/improvements.
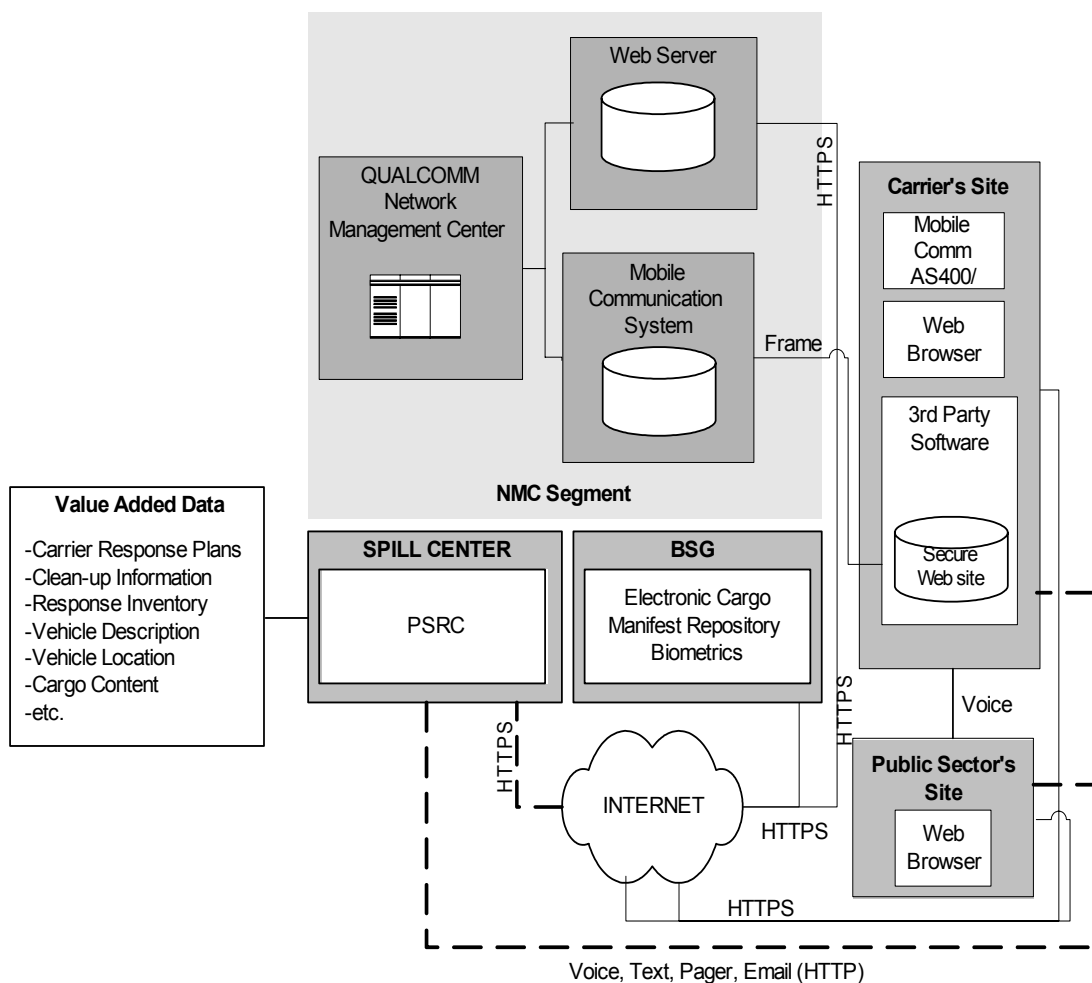
Figure 9-1. HAZMAT Public Sector FOT System Architecture.

9.3.2   Field Testing

Through tailored testing, the PSRC technology was applied to four existing FOT motor carriers involving FOT Requirements 2.2, 2.4, and 2.11.The tests' objective was to assess whether the PSRC systems adequately met the public sector functional requirements with respect to generating customized alerts and handling data generated and delivered as part of the larger FOT, and to identify improvements in timeliness of alert notification.

The Public Sector FOT involved four of the nine carriers participating in the full-scale HAZMAT and Security FOT. The Public Sector FOT also involved state law enforcement and response agencies from California, Texas, Illinois, and New York.

Testing for the Public Sector FOT was conducted onsite at locations within each of the four designated participant states during February and March 2004. The exact testing dates were as follows:

- February 4, 2004 in Houston Texas

- February 24, 2004 in Waterloo, New York

- February 26, 2004 at O'Fallon Inspection Station near O'Fallon, Illinois

- March 30, 2004 at Cox Petroleum in the City of Industry, California

Following is a description relating to the technology processes that were tested onsite for Functional Requirements 2.2, 2.4, and 2.11.

- **Requirement 2.2:** A state enforcement officer observed a driver performing the login procedure within the cab of the participant vehicle. To test the system, the driver purposefully failed the login process using Global Login or Biometric Login by exceeding the number of allowable login attempts without a successful login.

- **Requirement 2.4:** An "electronic fence" known as Geofencing was placed around a defined risk area or an exclusion zone. Alert notifications were triggered when the vehicle entered a prohibited area or when the vehicle leaves a predefined route. When a driver initiated a geofence violation, the polling rate, which is configurable to each specific motor carrier, was increased in frequency to track the vehicle's position, speed, and direction. Controlled tests were conducted where the driver purposefully violated pre-determined electronic fencing schemas.

- **Requirement 2.11:** This testing simulated a driver being involved in a compromising position such as a hijacking or theft. The driver pressed the in-dash Panic Button and/or the wireless remote panic. This pinpointed the location and time of the incident in order to aid dispatch and state authorities. The panic message was sent simultaneously to both the carrier dispatcher through the QUALCOMM NMC and the PSRC.

In-depth descriptions for the four individual on site tests are contained in **Volume III, Section 5: Public Sector Component**.

9.4   PUBLIC SECTOR EVALUATION FINDINGS

The evaluation effort for this test focused on testing the two SOW-stated Public Sector FOT hypotheses:

1. The response times for emergency and enforcement personnel to respond to a HAZMAT security or safety incident can be improved through the implementation of these technologies and the reporting center operational concept.

2. The quality of the information provided to first responders will improve through the implementation of these technologies and the reporting center operational concept.

9.4.1   HAZMAT Response Time Improvements

The first hypothesis is that the response times for emergency and enforcement personnel to respond to a HAZMAT security or safety incident can be improved through the implementation of these technologies and the reporting center operational concept. The hypothesis is accepted based on the data generated field testing experiences at the four on site locations and comments from law enforcement and emergency response personnel.

The explanation for accepting the first hypothesis is broken down according to sub hypotheses for Requirements 2.2, 2.4, and 2.11.

Requirement 2.2
In the past, positive driver identification typically required a trip to the police station, a process that would take an officer between 30 minutes to as much as 2 hours based on law enforcement estimates. The biometrics or Global Login allows the officer to perform an on-site driver verification using over-the-air communications with selected database interfaces within approximately 1 minute.

Requirement 2.4
Under current conditions, it is often impossible for an enforcement officer to determine if a certain motor vehicle is "off route" or near a location where it should not be. For carriers without Satellite Communications with any visual mapping capabilities or vehicle location tracking capabilities, it is very difficult to maintain consistent tracking of a vehicle to make sure that it stays "on route" or out of unauthorized areas as designated by the carrier.

During the exit interviews for the full-scale HAZMAT FOT, carriers were asked how long it would take them to determine that a vehicle was out of route without Satellite Communications. The motor carrier participants estimated it would take at least 4 to 8 hours on average to determine that a vehicle was where it should not be without Satellite Communications. Therefore, it would be at least 4 to 8 hours before law enforcement would be aware of an "off route" or geofence violation without Satellite Communications or Geofencing technology present.

At the standard 1-hour positioning frequency, Geofence technology routed through the PSRC and Satellite Communications to visually follow vehicle location progress provides a significant time benefits for law enforcement to detect an "off route" or Geofence violating motor vehicle. It can take up to 1 hour to for the system to detect an "off route" or geofence violation based on the standard 1 hour positioning frequency. Once this violation is detected, the alert message is sent out within 1 minute to authorized stakeholders, including the motor carrier management, dispatcher, law enforcement, and first responder personnel. This translates to at least a 3-hour time benefit of Geofencing delivered alerts through the PSRC and Satellite Communications for tracking vehicle location progress versus motor carrier vehicles not involving these technologies.

Requirement 2.11
Without being able to utilize a Panic Button to alert a dispatcher or law enforcement that a safety or security incident is taking place, at best, a driver can use a cell phone to communicate that situation. There are many situations when it would not be practical for a driver to communicate via a cell phone. The driver could be in the midst of a vehicle hijacking, where it would be impractical and actually dangerous to attempt to use a cell phone. The driver could also be in a "dead zone" where cell phone coverage is not available. Without a cell phone, the driver would have to wait to get access to another phone to report the incident – if and when the opportunity occurs. Even with a cell phone distress call to dispatch, the dispatcher would still have to determine, record, and relay all the location information to appropriate law enforcement channels to initiate response action.

The best estimate of response time to a "panic alert" is to use the average notification time for law enforcement response to a HAZMAT spill. Estimates based on Operation Respond and COMCARE place the estimate at 20 minutes. According to the Center for Technology Commercialization, the "best estimate" is 27 minutes.[44] A panic alert takes a maximum of 2 minutes to be routed to law enforcement through the PSRC. This represents at least an 18-minute time benefit to using Panic Buttons over average notification times at this time.

---

[44] The Center for Technology Commercialization(CTC) serves as NASA's Northeast Regional Technology Transfer Center (RTTC), covering the six New England States plus New York and New Jersey. CTC acts as a gateway for the transfer of NASA and other federal technology to private industry. The CTC's Public Safety Technology Center (PSTC) is an informational clearinghouse focused on the development and uses of advanced technologies that can help reduce violent crime, promote officer safety, and impact public safety's ability to effectively combat crime and respond to terrorist threats.

9.4.2   HAZMAT Information Improvements

The second hypothesis states that the quality of the information provided to first responders will improve through the implementation of these technologies and the reporting center operational concept. The hypothesis is accepted based on the law enforcement interviews and field testing public sector reactions at the four on site locations from law enforcement and emergency response personnel. The explanation for accepting the second hypothesis is broken down according to sub hypotheses for Requirements 2.2, 2.4, and 2.11.

Requirement 2.2
Currently, law enforcement typically relies on information provided by the subject for identification. The individual may choose to identify himself or herself using fraudulent identification credentials. It is difficult to remotely verify an individual's identity and only sketchy information is available without a reliable means to verify identification. An officer must depend on visual identification to make a decision as to an individual's identity. In the cases of unauthorized drivers, those individuals might have forged identification to pass themselves off as legitimate drivers.

The Biometric Login or Global Login provides much more accurate, truthful information on a driver during roadside enforcement actions. With laptop access in remote locations, law enforcement can verify driver identity, and with ESCM capabilities, ensure that the correct driver is associated with the correct vehicle/cargo. ESCM manifests detail the entire supply chain transaction from shipper pickup to consignee delivery. The law enforcement officer can determine who should be in control of a shipment at the point of the remote vehicle stop.

Requirement 2.4
Currently, law enforcement relies on the motor carrier to provide details for an "off route" or Geofence-violating truck. Law enforcement information is only as detailed as what the motor carrier provides. In cases where a carrier has no Satellite Communications, precise vehicle location is impossible with only a rough estimate based on travel times would be available. For details on cargo contents, without ESCM, law enforcement must contact the motor carrier, who may or may not have precise details on what is being hauled. In some cases, the shipper would have to be contacted by law enforcement for precise cargo contents to determine what real risk is posed by a particular off route or Geofence-violating truck, depending on what type of HAZMAT is being hauled. Different HAZMAT classifications carry different risk levels associated with their transport.

Geofence alerts contain a precise location of the alert event. Satellite tracking allows for continuing monitoring a vehicle once an alert is received at an increased positioning rate. The PSRC approach is to provide exception-based off route or Geofence alerts to law enforcement or first responders when there is a real defined emergency. Geofencing technology allows each route to be configured according to each specific shipment type, allowing for a precise risk level to be ascribed to each shipment and route. The PSRC allows for law enforcement or first responders to select what types of alerts to receive, and contact by a certain method (phone, e-mail, fax, page, etc.).

ESCM allows for law enforcement to know what cargo is on what truck when responding to an off route or Geofence alert to better assess risk. There is no need to contact the carrier to obtain load information – the information is contained on the manifest when it is electronically accessed.

The PSRC delivers precise, manageable information to law enforcement and first responders when dealing with off route or geofence violating trucks.

Requirement 2.11
Currently, law enforcement does not receive a real-time "panic alert". The best law enforcement can hope for is a cell phone call placed after the fact, to describe apparent location and what occurred during the event.

Panic Buttons provide an effective way to transmit emergency event information directly to law enforcement through the PSRC. Panic Buttons utilize Satellite Communications to pinpoint exact location and forward that location information to the NMC and to the PSRC and ultimately to end users such as law enforcement. There is no searching for location information pertaining to an emergency event that requires immediate response to a precise location.

9.4.3   Conclusion

As a proof of concept, the PSRC demonstrates the ability to fuse and disseminate critical HAZMAT information in a timely manner to enhance enforcement response to security events.

On a basic level, the PSRC system successfully demonstrated that as a system. The PSRC has the ability to improve:

- The response times for emergency and enforcement personnel to respond to a HAZMAT security or safety incident through the implementation of these technologies and the reporting center operational concept.

- The quality of the information provided to first responders through the implementation of these technologies and the reporting center operational concept.

In expanding the PSRC concept to a full deployment scenario, significant institutional/ procedural issues will need to be addressed. Among the more important of these is the administration of information and the notification process, i.e., ensuring that shipment information, alert notification levels (triggers), and key persons to be notified are current and complete. If not, the effectiveness of the system may be significantly eroded by alerts being directed to personnel or agencies that may not be involved in responding to given incidents, or that appropriate persons/agencies may not be alerted when actually warranted or that information provided is lacking or inaccurate. In either case, confidence in the PSRC and the ability to readily use alert and shipment background information provided via the PSRC is at stake. Addressing this will require coordination, continuity, and uniformity of processes among shippers/consignees, HAZMAT motor carriers and the enforcement/emergency response communities.

10. POLICY OPTIONS TO REALIZE DEPLOYMENT

The previous sections of this synthesis document described the test technologies in terms of performance in the field; how participating motor carriers and enforcement agencies used them; their impressions of effectiveness in improving operations and mitigate risk of terrorist activity, issues and concerns; and on return on investment (ROI) to private and publics sectors. The concerns of the participants are considered along with well-documented technology deployment issues of the motor carrier industry. These issues present barriers to full deployment of potentially beneficial technology systems. These issues are described in the following subsections.

10.1   ISSUES

10.1.1 Technology Cost

The predominant issue of the participating motor carriers and the enforcement agencies is "How will the systems be paid for?" For the motor carriers, the Wireless Communications with tracking capabilities was viewed as a positive ROI-generating technology, while few others tested were. In fleets such as Bulk Fuel and LTL-package delivery services that rely heavily on driver management to increase revenues and lower costs, in-vehicle login features were considered as an ROI-generating technology feature. Though not a revenue generator, the low-cost additional feature, the Panic Button, was considered a valuable security capability and one that would likely be readily adopted by fleets using the core communications capabilities. Other technologies tested were considered potentially useful and would be adopted if reliability of performance was high and if the customers demanded their use and were willing to accept higher freight rates to cover their expense. In other words, the carriers did not see salient reasons to invest in them unilaterally.

10.1.2 Technical Performance

An important issue identified is the technical reliability of systems, especially with respect to security. Overall, the commercially available technology systems performed as designed. It was observed during the test that the emerging technologies – E-seals, the Biometric identification systems, and the PSRC exhibited in the field shortcomings that will need to be addressed before they would be attractive commercially.

For the Biometric system, a Reader that is both accurate but forgiving in regards to how a driver places his/her finger on the device and what condition the drivers finger is in – greasy, wet, etc., is needed to prevent driver frustration with the inability to log into a vehicle. This is especially germane if future in-vehicle login systems are linked to the ability to start the vehicle.

For the E-seals, initially the system was slow in responding to arming and disarming commands, thus delaying the driver in his/her duties. A later software version improved the time lag, but still not to a convenient level for drivers. More importantly, it was observed that the seal could not be read through a "newer, heavy-duty" trailer, in which hundreds of thousands of units are already in service and is rapidly becoming the industry standard in dry van trailers. This is a technical issue that would need to be resolved or a potentially large portion of the market may not be realized.

The PSRC-staged events demonstrated the capabilities of the system to employ decision agents to screen and disseminate information across multiple distribution modes to

personnel in the field. A shortcoming of the technology system observed in a staged test in California was its reliance on cellular communications for distributing information. In areas where cellular coverage has a dead zone, the system was unable to forward alerts to the enforcement personnel.

Many motor carriers may delay investment in emerging technology concepts until systems are sufficiently field proven en mass.

10.1.3 Vendor/Product Stability

The purchase, installation, staff training, and system maintenance associated with technology acquisition represent significant investments for motor carriers. A valid business risk often described by Information Technology (IT) managers in transportation companies is whether product offerings will become "orphaned" (i.e., the vendor either exits the business line entirely and/or no longer provides technical support for a product). Additionally, the state-of-the-art in technology is changing at an increasing rate, potentially making systems functionally obsolete prior to recouping of investment.

10.1.4 Liability Issues

Vehicle disabling was also considered a strong security capability, but the issue of potential safety consequences associated with disabling a vehicle in a fast-moving, congested traffic area dampened enthusiasm for this technology. The potential liability rests not only with all those who may initiate a vehicle disablement (carriers and enforcement), but also for those who are responsible for the vehicles.

On the opposite side of the issue is the potential liability if a truck is equipped with vehicle disabling technology or other security technology, and the technology is not activated in a timely enough manner to thwart an attack in that case.

Another liability issue that could arise for late adopters of a security technology is when a technology is so widely adopted that it becomes a defacto security standard. Should a carrier choose not to employ the technology, the carrier may be held liable if an event occurs that might have been stopped had the technology been in place. The threat of potential litigation can dampen the deployment of the technologies.

10.1.5 Data Privacy Issues

Given the extremely competitive nature of the motor carrier industry, operational data is extremely well guarded to prevent competing entities from obtaining a business advantage. Information regarding customers, routes, and cargo/quantities hauled, operational costs, and revenues are key to managing a fleet and establishing and maintaining a customer base founded on rates and service. However obtained, this information could allow a competitor to undercut prices and steal business from a carrier. On the security side, the less information that could be obtained by a terrorist cell regarding carriers' operations, the less likely a successful attack could be planned and mounted.

From a potential litigation point of view, detailed operational data that the test technologies are capable of collecting and archiving are at risk of disclosure in legal actions following an incident, whether due to traffic collision or terrorist activity. Providers of tracking and other telemetry collection and transmission services have responded with contractual agreements with customers regarding the length of time for archiving records and information accessibility. This notwithstanding, archived motor carrier data may still be at risk.

With regard to the public sector, there has been a long-standing reluctance to make proprietary data accessible. This reluctance is based in concerns about limits of use within government and the potential access to data by other entities under laws such as the "Freedom of Information Act". Regarding use of data within government, carrier concerns focus on information being used to facilitate or enable additional tax structures, set policy and regulations, or instigate enforcement actions against carriers. This can be particularly germane to the PSRC concept in tracking vehicles or accessing archived manifest data via ESCM.

10.2   POLICY OPTIONS FOR OVERCOMMING ISSUES AND REALIZING INDUSTRY DEPLOYMENT

There are several possible strategies that could be employed singularly or in combination to stimulate industry deployment of technologies that show promise for reducing vulnerabilities in truck-based HAZMAT shipping.

For nearly all motor carriers, return on investment is the lead factor in the adoption of technology systems. As found in this FOT, many of the technologies tested did not demonstrate a quantifiable improvement in motor carriers' bottom line, but did show promise for reducing vulnerabilities in truck-based HAZMAT shipping, and therefore, rendering potentially significant societal benefits. In establishing policy, the government needs to weigh these potential societal benefits against the possibility of negatively impacting the trucking industry's ability to move freight efficiently and profitably.

Therefore, combinations of strategies can be employed by the government to encourage accelerated deployment of promising technologies. Several of these (in no particular priority order) are described in the following subsections.

10.2.1 Technology Cost

To address technology cost issues, the following policy options are proffered:

1. Develop outreach to motor carriers describing potential efficiency and security benefits.

2. Work with motor carriers and technology vendors to encourage cooperative purchasing arrangements to take advantage of volume discounts.

3. For public sector agencies, investigate the feasibility of using current funding mechanisms such as the Motor Carrier Safety Assistance Program (MCSAP) for deploying PSRC-enabling technologies.

10.2.2 Technical Performance

To address technology performance issues, the following policy options are proffered:

1. Collect and promulgate long-term data to accurately quantify technical reliability in many operational environments.

2. Encourage vendors to include motor carriers in the process of new product design.

10.2.3 Vendor/Product Stability

The issue of vendor/product stability can be addressed through outreach by encouraging motor carriers to be aware of the changing market place for ITS products and services. The outreach could provide a directory of organizations such as ITS America from which carriers can obtain information.

10.2.4 Potential Liability Issues

To address liability issues, the following policy options are proffered:

1. Research potential legal issues associated with the purchase and use, or lack thereof, of security-oriented technologies. This would establish a baseline assessment of liability risk and its contributing factors.

2. Define limits on acquisition of archived motor carrier data.

3. Establish well-defined criteria for enforcement escalation and intervention procedures.

10.2.5 Data Privacy Issues

To address data privacy issues, the following policy options are proffered:

1. Review policies and laws regarding public access to proprietary company information to enable legislation, policies and procedures to appropriately protect competitively sensitive information.

2. Establish clearly defined limits on the use of motor carrier information and sharing among government entities.

11. CONCLUSIONS

This complex HAZMAT Safety and Security Technology Field Operational Test was conducted in the pursuit of improving Homeland Security vis-à-vis protection of truck-based hazardous materials shipments. With over 800,000 HAZMAT shipments per day with the staggering potential consequences in terms of deaths, injuries, property damage, and business disruption of even one shipment used by terrorists for an attack the immediacy of implementing countermeasures rapidly is obvious. With resources in limited supply and many counter-terrorism fronts to contend with, meeting the "clear and present danger" to HAZMAT trucking requires implementing solutions that are currently available, reduce risk, and that provide tangible and quickly realized benefits to stakeholders proportional to their level of investment.

This evaluation examined the technical and financial performance of several promising technologies for increasing the security of HAZMAT shipments to determine what levels of operational efficiency and security benefits can be attained through deployment of the technologies. The evaluation also examined the levels of investment required to equip fleets with the technologies. Based on the evaluation of the test technologies, the following conclusions are presented in Sections 11.1 through 11.6 of this synthesis document.

11.1   TECHNICAL EFFICACY

Technology performance overall for the technologies was good, with most technologies performing well under operational conditions with the exception of Biometric Login, and to a lesser Electronic Seals and ESCM. These latter two technologies were deemed as requiring additional technical development for the HAZMAT trucking environment.

The core enabling technology for the test suites, Wireless Communications with GPS tracking capabilities, has been deployed commercially for several years and performed per expectations during the FOT. The technology also demonstrated its ability to integrate additional security functions with the established communications network providing a reliable data transfer mechanism.

The Panic Button, vehicle disabling, trailer tracking, and Geofencing applications of the core enabling technologies also performed per specification.

As described in this synthesis document, the Biometric identification units supporting Biometric driver logins and access to the ESCM need to be more "forgiving" for climatic conditions and physical application of drivers' fingers to the Readers. The E-seal system, even after undergoing modification during the FOT, showed cycle times considered too long by the participants. Additionally, a more user-friendly software interface is recommended. The ESCM, as demonstrated in a previous test of application and during this FOT, requires the development of interfaces with other systems used by motor carriers. The integration of ESCM with carrier systems would increase usage of the system.

11.2   EFFICIENCY

The core enabling technology is the only technology tested that demonstrated tangible operational efficiency gains within the limits of this FOT. Productivity gains in terms of increased personnel and asset utilization are found to outweigh the costs of deploying the technology with relatively attractive payback on investment periods. With the proven

reliability of the technology in the market place and appropriateness of application to a wide range of fleets significant industry benefits could be realized through full deployment-with net benefits over costs of up to $1 billion per year. Even with attractive ROI and low payback periods, capital constraints, institutional inertia (comfort with doing business in fixed ways), and myriad low- cost communications options are likely to make penetration of this market a long-term enterprise, especially in the smaller fleet categories.

11.3   SECURITY

The technology suites tested during the FOT, given further development (as described for the "emerging" technologies – those not commercially available for the HAZMAT trucking market) show promise for significantly reducing vulnerabilities and hence, reducing potential impacts of terrorist attacks. It should be recognized that technology alone, at best, could only address approximately one-third of the potential HAZMAT-based consequences.

The core enabling technology also provides significant security benefits. The implication is that the core enabling technology has the capability of more than covering its costs to motor carriers while providing a significant security benefit to society. Given this, policy makers should consider how best to further reduce costs through several possible mechanisms and promulgate information to motor carriers.

The remaining technologies do show considerable potential security benefits (societal benefits), but not necessarily realized by the motor carriers, such as both the E-seal and OBC with door lock are potential security improvements in the attempt to bolster en transit cargo protection. Both technologies in theory enable remote detection of an intrusion of the trailer by an unauthorized party at any point from pick up to delivery of cargo and to some extent make it more difficult for entry into the trailer.

Therefore, decision makers need to weigh the potential investment versus additional security benefits for the technologies and if deemed desirable, then work with the HAZMAT industry (shippers, carriers and consignees) to move towards deployment in an equitable fashion.

11.4   SAFETY

The benefits of the technologies as deployed, focus on enhanced driver monitoring capabilities, reduced exposure to crashes, and enhanced HAZMAT incident response. Within this framework, participant opinion indicates that the technical capabilities of the test technologies, coupled with best practices in motor carrier driver/safety management and public sector incident response, show promise for enhancing the safety of truck-based HAZMAT shipments. The technologies demonstrated enhanced ability to monitor drivers and vehicles and provide notification of emergencies with location and load characteristics in a more timely manner and potentially detailed manner than traditional methods (thus, potentially enhancing emergency response).

Through enhanced fleet management enabled by the core technology of Wireless Communications with GPS positioning, fewer non-revenue miles can be realized. Assuming these miles translate directly to fewer overall miles driven, potential benefits in terms of crash avoidance due to reduced exposure were conservatively estimated to be $5 million annually.

11.5   DEPLOYMENT POTENTIAL

As described in the previous sections, the core enabling technology for the test suites has the capability to enhance motor carriers' operational efficiencies and generate benefits in excess of deployment costs. Recognition on the part of the technology vendor community of the variability in the needs of HAZMAT trucking operations and responding by providing the basic core functions adapted to specific types of operations and at a range of pricing/financing options should drive motor carrier adoption of the technology and make it a prevalent fleet management technology in the future. This market-based move towards increased market penetration may be at a less robust pace than the increasing need of securing truck-based HAZMAT shipments. In this case, governmental intervention (discussed as policy options in Section 10.2 of this synthesis document) may be required.

For the technologies that build upon the core technology, market forces are unlikely to support strong adoption of the technologies, at least in the foreseeable future. A possible exception may be imposition of requirements for technology imposed by shippers/consignees that would create a "derived demand" on the part of HAZMAT trucking operations to adopt the technologies.

11.6   PUBLIC SECTOR PSRC CONCEPT

As a "proof-of-concept" system, the PSRC provides a model for enhanced information exchange between public and private sector HAZMAT stakeholders by providing law enforcement and emergency response personnel access to accurate, timely, and action-oriented information. As a solution, the PSRC system holds the potential to enable law enforcement and emergency response personnel to respond to intentional and unintentional incidents associated with the transportation of hazardous materials.

For future PSRC or similar system concept testing the following elements should be considered as enhancements to the current PSRC concept:

- A robust, standardized central data repository for data storage and retrieval must be created with built in redundancy for information collection, fusion and dissemination.

- An effective interface must be developed to filter data to ensure that sensitive or corrupt data remains outside of any data delivery through the PSRC. As the recipient of key information, the PSRC must forward only critical information to public sector users in a prioritized and easy to manage format, which can be easily integrated with their current systems.

- The PSRC serves as the link between data sources collecting the initial data on one end and delivering the alert notification data on the other. On the data collection side, mostly private carrier data is the primary source data for the PSRC at this point. In the future, it may be desirable to include information from sources (criminal databases, state commercial vehicle systems, terrorism watch lists, etc.) that might provide in-depth information relevant to criminal or security activity.

11.7   POLICY OPTIONS

As described in Section 10 of this synthesis document, significant issues exist that need to be addressed to move towards deployment of the promising security technologies. Governmental strategies that can be employed to encourage deployment include:

- Support of research and development for adoption of commercially available and emerging technologies that show promise for enhancing security through continued field testing. This support can involve extending the testing conducted in this FOT over time and across a larger number of motor carriers.

- Creation of financial incentives to encourage research and development and purchase of technologies such as grants or facilitating cooperative purchasing arrangements.

- Legislative and procedural action to address data privacy issues.

- Promote technology acceptance through focused outreach and public relations efforts.

- Craft regulation/rulemaking requiring the adoption of solutions to address HAZMAT trucking vulnerabilities. These should be performance-based requirements that provide motor carriers flexibility in how they meet the requirements.

REFERENCES

- ATA Foundation, Motor Carrier Technologies – Fleet Operational Impacts and Implications for Intelligent Transportation Systems/Commercial Vehicle Operations, October 1999.

- ATA Foundation, NAFTA Priority Corridor Comprehensive ITS/CVO Plan Motor Carrier Technology Survey, August 2000; American Transportation Research Institute – GartnerG2, Trucking Technology Survey, 2003.

- ATRI – GartnerG2 Trucking Technology Survey, December 2002.

- ATRI – GartnerG2 survey of 150 motor carriers on adoption of in-vehicle technologies, Trucking Technology Survey – 2003; ATRI industry survey of 348 motor carriers to determine levels of technology adoption in 2000 and projections to 2003, in support of the North American International Trade Corridor (NAITC) Comprehensive and Coordinated Intelligent Transportation Systems for Commercial Vehicle Operations (ITS/CVO) Plan, 2003.

- ATRI, Trucking Technology Survey, conducted as part of the FOT, Hazardous Materials Security and Technology Survey Results Summary, January 2004.

- Battelle, in association with QUALCOMM, ATRI, CVSA, and the Spill Center, HAZMAT Safety and Security Field Operational Test Draft Final Report, June 11, 2004.

- Battelle, HAZMAT Safety and Security Field Operational Test: Task 2: Concept of Operations, prepared for FMCSA, April 18, 2003.

- Battelle, HAZMAT Safety and Security Field Operational Test: Task 4 System Requirements and Design. May 1, 2003.

- Battelle, Framework for Assessing Safety & Security Incident Consequences for Highway Shipments of Hazardous Materials, Final Report prepared for the USDOT and FMCSA, December 2003.

- Battelle, *HAZMAT Field Operational Test Task One: Conduct A Risk/Threat Assessment*, Draft Report prepared for the U.S. Department of Transportation (USDOT), Federal Motor Carrier Safety Administration (FMCSA), October 2002.

- *Federal Register* / Vol. 68, No. 86 / Monday, May 5, 2003 / Rules and Regulations, p. 23867.

- Figure derived from the USDOT Bureau of Transportation Statistics, Motor Carrier Finance and Operating Statistics.

- FMCSA Analysis Division, Large Truck Crash Facts – 2002, 2001, 2000.

- Kansas Department of Transportation, Incident Management Program Background, Spring 2002.

- Nicholas J. Garber and Lester A. Hoel, Traffic and Highway Engineering, PWS Publishing, New York, New York, 1999, page 153.

- People's Daily Online, October 5, 2001.

- SAIC, Hazardous Material Transportation Safety and Security Field Operational Test Final Detailed Test Plans, prepared for FMCSA, September 2003.

- Triantaphylou, Evangelos and Lin, Chi-Tun, "Development and Evaluation of Five Multi-Attribute Decision Making Methods", International Journal of Approximate Reasoning, 1996, Volume 14, pp. 281-310.

- The Volpe Center, Surface Transportation Vulnerability Assessment, October 25, 1999.

- USDOT Bureau of Transportation Statistics, Motor Carrier Finance & Operating Statistics, 2002, accessed from http://transtats.bts.gov/.

- U.S. Government Accounting Office, GAO-02-700R, *Impact of Terrorist Attacks on the World Trade Center*, May 29, 2002.

- U.S. Office of Management and Budget-Circular No. A-94 – Appendix C – Discount Rates for Cost Effectiveness, revised February 2004.