NOTICE: This document has been approved for public disclosure. Appendix E containing Sensitive Security Information has been removed. References to this appendix remain in the document.

HAZMAT SAFETY & SECURITY FIELD OPERATIONAL TEST

FINAL REPORT

To

Federal Motor Carrier Safety Administration
U.S. Department of Transportation
Washington, DC 20590

Battelle
The Business of Innovation

In association with:

Qualcomm

American Transportation Research Institute

Commercial Vehicle Safety Alliance

Spill Center

August 31, 2004

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-OP-03-XXXX		

4. Title and Subtitle	5. Report Date
Hazardous Material Transportation Safety and Security Field Operational Test (FOT) Final Report – Deployment Team	August 31, 2004
	6. Performing Organization Code
7. Author(s) D. Williams (Battelle), J. Allen (Battelle), M. Lepofsky (Battelle), D. Murray (ATRI), K. Wahl (ATRI), D. Vercoe (QUALCOMM), S. Keppler (CVSA), T. Moses (Spill Center)	8. Performing Organization Report No.
9. Performing Organization Name and Address Battelle 505 King Avenue Columbus, OH 43201-2693	10. Work Unit No. (TRAIS)
	11. Contract or Grant No. DTMC75-01-D-00003, TO 5
12. Sponsoring Agency Name and Address **U.S. Department of Transportation** Federal Motor Carrier Safety Administration 400 7th Street, S.W. Washington, D.C. 20590 Intelligent Transportation Systems – Joint Program Office 400 7th Street, S.W. Washington, D.C. 20590	13. Type of Report and Period Covered
	14. Sponsoring Agency Code

15. Supplementary Notes

Mr. Joseph DeLorenzo (FMCSA) (COTR)
Ms. Kate Hartman (USDOT/JPO)

16. Abstract

See text of document

17. Key Word	18. Distribution Statement
Hazardous Materials; Intelligent Transportation Systems; Security; Field Operational Test; Technology Evaluation; National Test; Emergency Responders; Public Sector Reporting Center;	Distribution of this document (with the exception of Appendix E) is unrestricted. Distribution of Appendix E of this document is considered Sensitive Security Information (SSI) and distribution is restricted without written permission from the US DOT. The non-SSI portion of this document is available to the public from: The National Technical Information Service, Springfield, VA 22161

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Appendix E – SSI	Unclassified	165	N/A

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

Table of Contents

Table of Contents (Continued)

Table of Contents (Continued)

List of Appendices

Table of Contents (Continued)

Page

List of Tables

Table of Contents (Continued)

Page

List of Figures

Abstract

This report summarizes the deployment activities associated with the United States Department of Transportation (USDOT) Federal Motor Carrier Safety Administration's (FMCSA's) Hazmat Safety and Security Field Operational Test (FOT). The FOT was conducted over a 24-month period, beginning in September, 2002 and culminated in a six-month field testing of multiple technologies. The purpose of the FOT was to quantify the security costs and benefits of an operational concept that applies technology and improved enforcement procedures to hazmat transportation and was scoped to address the following risk areas: driver verification, off-route vehicle alerts, stolen vehicles (both tractors and trailers), unauthorized drivers, cargo tampering, and suspicious cargo deliveries.

The FOT was centered around deploying technologies that addressed the 23 separate functional requirements established by the US DOT.

As part of the Hazmat FOT, a risk/threat assessment (Task 1) was conducted to organize the safety and security risks and threats in the highway transportation of hazardous materials. That report framed the safety and security risks being addressed by the FOT and was the basis (along with the RFP requirements and the Battelle Team's proposal) for developing the Concept of Operations (Task 2).

The general approach to conducting the FOT was centered on breaking the FOT into four operational scenarios. Each scenario addressed different segments of the hazmat transportation market. As such, each scenario deployed a different "suite" of technologies. The technologies deployed by scenario were selected based on several key factors:

- The technologies selected must account for the unique characteristics of each segment of the hazmat marketplace (long-haul, short-haul, pick up and delivery, etc.)

- The impact of using the technologies (cost, security) must be appropriate for the operational characteristics of the market segment. For example, munitions and explosives carriers are typically long-haul, for-hire carriers and may be required to have communications and tracking capabilities. In contrast, the short-haul petroleum segment generally involves local fleets, working from a centralized dispatch and operating on thin profit margins and are not required to have the communications and tracking capabilities. Thus, technological solutions to the security issues must take into account the operating environment and the need to minimize the costs of the solutions.

- A goal to address all the functional requirements identified by DOT.

The installation and field testing of technologies was spread over nine months (six-month operational period with staggered start/stop dates at each carrier), involved participation of nine different commercial hazmat carriers, multiple shippers and consignees and law enforcement/ emergency responder agencies from four states (New York, Illinois, Texas and California). This report documents the activities, lessons learned and recommendations of the FOT deployment team. A separate independent evaluation was conducted (lead by SAIC) and a final Evaluation Report will be prepared and published separately.

Acknowledgements

The Hazardous Materials Safety and Security Field Operational Test (FOT) was conducted under the auspices of the Federal Motor Carrier Safety Administrations' (FMCSA) Hazardous Materials Division and was managed by Joseph DeLorenzo. The operational test was a joint effort by FMCSA, the Federal Highway Administration (FHWA), and the U.S. DOT – Intelligent Transportation Systems Joint Program Office.

Battelle led the deployment team that designed and implemented the test. The other team members included Qualcomm, the American Transportation Research Institute (ATRI), the Commercial Safety Vehicle Alliance (CVSA), Saflink[1], Savi Technology, The Spill Center, and Total Security Services International (TSSI).

A strong group of industry and state partners contributed to the success of the operational test. This group included carriers, shippers, consignees, and state motor carrier enforcement agencies. All of these organizations volunteered their time, personnel, and commitment to fulfill their roles as participants. We offer our sincere appreciation for their involvement.

Carriers: Dupre Transport, Cox Petroleum, Distribution Technologies, Roadway Express, Transport Service, Quality Distribution, Roeder Cartage, R&R Trucking, and Dyno Transportation

Shippers: ExxonMobil, GE Betz, DOW Chemical, BP Chemical, Orica USA, and Dyno Nobel

Consignees: NuFarm Americas, Evans Chemical, Orica USA, Dyno Nobel

State Agencies: Texas Department of Public Safety, California Highway Patrol, Illinois State Police, and New York State Police

Special recognition should also be extended to the members of the Hazardous Materials Review Team, established to provide overall guidance and direction to the deployment team.

[1] Note: In previous documents produced as part of this FOT, Saflink was referred to as Biometric Solutions Group (BSG). Saflink purchased BSG during the FOT.

Deborah Freund
Federal Motor Carrier Safety Administration

John Lambert
Research and Special Programs Administration

Kate Hartman
U.S. DOT – Intelligent Transportation Systems Joint Program Office

Jeff Loftus
Federal Motor Carrier Safety Administration

Amy Houser
Federal Motor Carrier Safety Administration

Bill Quade
Federal Motor Carrier Safety Administration

Kevin Johnson
Transportation Security Administration

Pierre Yousef
Mitretek

We appreciate the valuable input provided by the External Stakeholder Review Group. These volunteers from the shipper, carrier, and enforcement communities helped to expand the range of viewpoints and perspectives that were considered during the course of the operational test.

Al Roberts, Chair
Dangerous Goods Advisory Council

Captain Bruce Bugg
Georgia Department of Motor Vehicle Safety

Gary Briese
International Association of Fire Chiefs

Cynthia Hilton
Institute of Makers of Explosives

Richard Barlow
Lyondell Chemical Company

Final recognition goes to the deployment team members and the primary authors of this report:

John Allen
Battelle
Project Manager

Dan Murray
ATRI

David Williams
Battelle
Operations Manager

Katie Wahl
ATRI

Mark Lepofsky
Battelle

Derrick Vercoe
QUALCOMM, Incorporated

Stephen Keppler
CVSA

Tom Moses
The Spill Center

Christina Jin
Saflink

Jeff Beaty
TSSI

Jerry Bredeson
Savi Technology

Acronyms

ATRI	American Transportation Research Institute
BP	British Petroleum
CDL	Commercial Driver's License
COTS	Commercial-off-the-shelf
CPU	Central Processing Unit
CSR	Customer Service Representative
CVO	Commercial Vehicle Operations
CVSA	Commercial Vehicle Safety Alliance
DAG	Hazmat Direct Action Group
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DSRC	Dedicated Short-Range Communication
DOT	Department of Transportation
E-Manifest	Electronic Manifest
ESCM	Electronic Supply Chain Management
FBI	Federal Bureau of Investigation
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FOT	Field Operational Test
FR	Functional Requirement
GPS	Global Positioning System
Hazmat	Hazardous Materials
HM	Hazardous Materials
HTA	Heavier-than-Air
IACP	International Association of Chiefs of Police
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
LTA	Lighter-than-Air
LTL	Less-than-Truckload
MCMIS	Motor Carrier Management Information System

MCT	Mobile Communications Terminal
NMC	Network Management Center
OBC	On-board Computer
P&D	Pickup and Delivery
PDA	Personal Digital Assistant
PSRC	Public Sector Reporting Center
RFID	Radio Frequency Identification Device
ROI	Return on Investment
RSPA	Research and Special Programs Administration
SAFE	Security Awareness for Enforcement
SAIC	Science Applications International Corporation
SRD	Systems Requirement Document
SSI	Sensitive Security Information
TIH	Toxic-by-Inhalation
TSSI	Total Security Services International
TL	Truckload
U.S. DOT	U.S. Department of Transportation
VIUS	Vehicle Inventory and Use Survey
WPB	Wireless Panic Button
WVD	Wireless Vehicle Disable

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) and the Intelligent Transportation Systems (ITS) Joint Program Office (JPO) within the U.S. Department of Transportation (U.S. DOT) sponsored a major field operational test (FOT) to assess the potential enhancement of the safety and security of hazardous materials transportation resulting from the application of various technologies. The Hazardous Materials Transportation Safety and Security Field Operational Test program was conducted from August, 2002 to August, 2004. The goal of the FOT was to demonstrate and assess the effectiveness of certain technological solutions for enhancing the safety and security of hazardous materials transportation by highway

In the aftermath of the terrorist attacks on September 11, 2001, there was extremely heightened concern about the potential for terrorists to highjack a truck carrying hazardous materials or use it in some other fashion to commit a terrorist act. FMCSA made over 32,000 contacts and security sensitive visits with hazardous materials carriers. These contacts and visits resulted in over 280 findings of "suspicious activity" and over 125 referrals to the Federal Bureau of Investigation (FBI). FMCSA identified an important potential role for technology to help improve motor carrier hazmat security. This was the result not only of the findings from the motor carrier security visits, but also from working with internal DOT working groups including the Intermodal HM Task Force and the Hazmat Direct Action Group (DAG). The internal DOT evaluation of hazmat security vulnerabilities identified a number of action items and initiatives across DOT. One major initiative was the need to take a close look at commercially available, off-the-shelf technology that could be deployed in the near term to help fill some of the most glaring gaps in hazmat transportation security. This led to a competitive solicitation to field test and evaluate appropriate technologies and the selection of Battelle to lead the deployment team in August, 2002.

The Deployment Team

Battelle served as the prime contractor, program manager and system integrator for this project. Battelle assembled and led a "core team" of partners to address FMCSA's requirements. This core team included Qualcomm, the American Transportation Research Institute (ATRI), formerly the American Trucking Association Research Foundation, the Commercial Vehicle Safety Alliance (CVSA) and Total Security Services International, Inc. (TSSI). The core team served as a central project planning group that set direction and responded to problems and issues as the project unfolded. The rest of the team involved technology providers for the test. Technology providers included Qualcomm, providing the wireless communication backbone and other technologies; Saflink providing the biometric smart card and electronic supply chain manifest technology; Savi Technology, Inc., providing its electronic cargo seal; and the Spill Center providing its integrated reporting system technology as the backbone for the public sector reporting center (PSRC) concept.

The Battelle deployment team included two organizations that represented the perspective of important stakeholders during the project (ATRI and CVSA), and the FOT included direct participation from six hazmat shippers, nine motor carriers, four consignees, and six state agencies in four states. In addition, a voluntary External Stakeholder Review Group was formed

with selected members of the shipper, carrier, and enforcement communities and met periodically to review progress of the operational test and offered comments and opinions.

Framework to Conduct the Test

DOT provided the overall framework for the field test as part of its contractual scope of work. This is illustrated in Figure ES-1. The test was to include consideration of technologies that addressed potential vulnerabilities during the pickup, en route and delivery phases of a hazmat shipment. This framework embraced 25 specific functional requirements initially identified by DOT to be addressed during the test. DOT specified that the test was also to address four shipment scenarios, at least 100 trucks, four motor carriers, a total of 100 tractor-trailer units, four shippers, four receivers, and HM industry and state safety enforcement representatives.

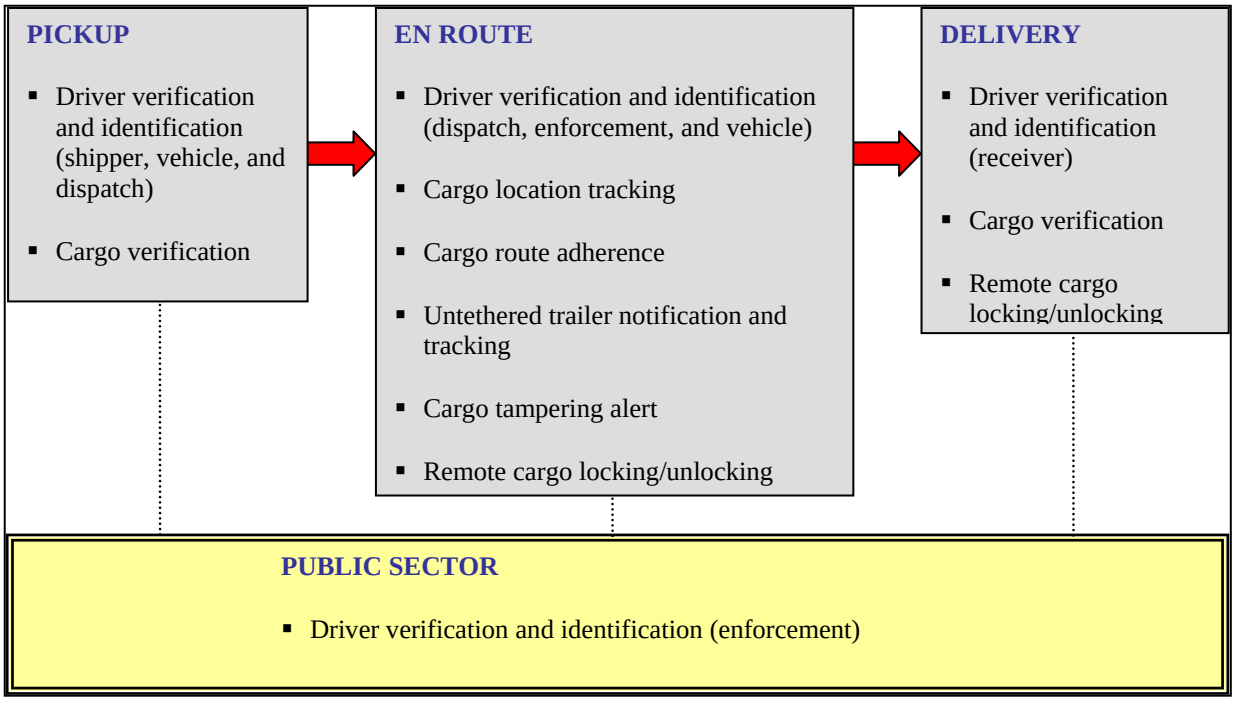

Figure ES 1: DOT Framework for FOT

Initial Assessment of Risks, Threats and Vulnerabilities to Validate Research Objectives and Calibrate Operational Scenarios to be Tested

Although DOT had provided this initial framework for the deployment testing, Battelle was asked conduct a high-level risk/threat assessment of hazmat transportation to ensure that this framework would fully satisfy the original research objectives. The assessment was to frame the safety and security risks being addressed by the operational test, calibrate the operational scenarios originally proposed, and to help prioritize technology countermeasures to be tested. A more detailed discussion of the risk and threat assessment is presented in Sections 3 and 4 of this

report and a much greater level of detail can be found in the Task 1 Project Report (see references in Section 6.0).

Battelle identified terrorist tactics that could be effective during the transportation of hazardous materials. These tactics, called attack profiles, drew upon a comprehensive database of threats developed by TSSI. Three key threats were identified: theft, interception (including diversion), and legal exploitation. These attack profiles were then mapped against the four shipment scenarios developed as part of the Battelle Team's initial planning efforts to ensure that all of the attack profiles would be addressed in the proposed field test plans. Also, over 30 specific vulnerabilities were identified during the analysis and estimates were made of potential consequences of successful terrorist events. These consequence estimates were then used to rank the threat and hazmat categories of greatest concern. Finally these rankings were used in finalizing the operational scenarios and associated technology countermeasures that were selected for testing for the field operational test.

Selection of Technologies to Address Research Objectives and Perform Operational Scenarios

Battelle worked with the rest of the deployment team and the DOT to select the technologies that would address the research objectives and that could apply to the four operational scenarios selected based upon the risk/threat assessment task. In selecting the technologies to test, it was important that the technologies be as close to commercial-off-the-shelf (COTS) as possible. While it was not an absolute requirement that all technologies be commercially available at the time of the FOT, it was important that the technologies be more than just a concept or early beta-test candidate.

The selected technologies are reviewed briefly here and discussed in detail in the body of the final report.

- *Communication System* – These included satellite and terrestrial communications with global positioning system (GPS) and tracking capabilities, and digital mobile phone technologies without GPS.

- *Panic Buttons* – An emergency alert message was generated via the use of a panic button, which came in two configurations: 1) a panic button mounted inside the vehicle to send an emergency alert, and 2) 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.

- *Driver Identification and Authentication System* – Two separate technologies were selected to authenticate drivers. First, Driver Authentication with Global Login, similar to a username and password on a computer system. Second, Driver Authentication with Biometric Verification was tested.

- *Electronic Supply Chain Manifest (ESCM) System* – Electronic manifesting was tested using biometric fingerprint readers to restrict unauthorized system access and validate driver identification.

- *Remote Vehicle Disabling* – An on-board computer (OBC) was used to control the disabling of the vehicle in a variety of means. These methods included blocking fuel, or sending proprietary system instructions via the wireless communications system directly to the vehicle's data bus.

- *Remote Cargo Door Locks* – Required the driver to request authorization from the carrier's dispatcher to lock or unlock the trailer door using over-the-air communications.

- *Electronic Cargo Seals* – This technology automatically generated an alert if the cargo seal was broken without proper authorization. The seal used short-range wireless communications to interface with a mobile E-Seal reader (located in the vehicle).

- *Geofencing* – This technology included specialized software that allowed the operator to set an "electronic fence" around any given route or point on a displayable map with automatic alert function if violated.

- *Trailer Tracking* – The trailer tracking subsystem provided untethered trailer position information to the dispatcher on a regular basis.

- *Public Sector Reporting System (PSRC)* – The Battelle Team created the PSRC in order to provide law enforcement with real-time hazmat alerts. A center was staffed live, 24/7, and was able to incorporate wireless voice/data communications, satellite-tracking technology, automatic routing of alerts to authorities, and online access to highly specialized data.

Operational Scenarios and Selected Technologies

Based upon the risk/threat assessment and the technologies selected for the test, the Battelle deployment team mapped specific technologies to the operational scenarios as shown in the table below. This became the foundation of the operational test upon which the concept of operations, requirements analysis, and system design for the FOT were based.

Table ES-1: Technology Components by Scenario

Scenario	Description	Technology Components	
1	Bulk Fuel Delivery	• Wireless Satellite Communication • Global Login • In-Dash Panic Button • Wireless Panic Button	• Digital Phone • Terrestrial Communication • On-Board Computer • PSRC
2	LTL High Hazard	• Wireless Satellite Communication • Global Login • In-Dash Panic Button	• Wireless Panic Button • Terrestrial Communications
3	Bulk Other	• Wireless Satellite Communications • Biometric Verification • In-Dash Panic Button	• Wireless Panic Button • Electronic Supply Chain Manifest • PSRC
4	Truckload (TL) Explosives	• Wireless Satellite Communication • Biometric Verification • In-Dash Panic Button • Wireless Panic Button • Electronic Supply Chain Manifest	• On-Board Computer • Wireless Electronic Cargo Seal • Geofencing • Trailer Tracking (Tethered and Untethered) • PSRC

Planning and Conducting the Field Test

The planning process to prepare for and execute a successful field operational test is critical. Over a period of approximately six months, from the fall of 2002 through the spring of 2003, the Battelle team conducted all of the planning and system engineering tasks required by DOT including the Concept of Operations, System Requirements Analysis, and System Design (see references in Section 6.0 for each task report). This was absolutely necessary for an effective test. In addition, the Battelle team conducted substantial outreach and training activities with the myriad of participants including carriers, shippers, receivers, and state enforcement staff. The training and outreach visits were conducted during summer and fall of 2003 as a prelude to the beginning of the operational test.

The Battelle Team conducted a beta test of the FOT on July 14-18, 2003 at Qualcomm headquarters in San Diego, CA. The beta test utilized the Qualcomm technology truck and included members of the Deployment Team and the Independent Evaluation Team, led by Science Applications International Corporation (SAIC). A full description of the beta test is presented in the full report. The FOT system design documents were modified as a result of the beta test and full-scale deployment of the FOT occurred between August 2003 and May 2004. Throughout the field test, there was close integration with the independent evaluators

During the field operational test, a variety of data was collected from the deployed technologies. Well over one million data points were collected. The type and format of data was refined several times based on initial data analysis conducted during the 2003 Beta Test. A data distribution plan forwarded all data to the Battelle research team, FMCSA, and to SAIC, the project's Independent Evaluation Team. Prior to distribution, a joint ATRI/SAIC data group continually analyzed data and questions and/or issues, and worked with the data system integrators and vendors to clarify or revise data presentations, or investigate system usage. Data was collected on a monthly basis.

Not all technologies produced "operational" data streams. Several technologies were tested both in staged testings in-person and during company visits.

Battelle, Qualcomm and the rest of the deployment team successfully conducted the field tests for all technologies identified for each of the operational scenarios. Detailed test plans were carried out to test the performance of technology applicable to each of the 25 functional requirements defined by DOT as part of the field test (see Section 4.5 of the full report for detailed descriptions

The Battelle deployment team spent considerable time and effort to ensure that adequate data was collected and provided as requested by the independent evaluator, SAIC. This test data will form the basis of the independent assessment of the Hazmat Safety and Security Operational Test.

Development of the Technology Compendium

One major task conducted as part of this project was to develop a compendium of technology in the marketplace that could have application to hazmat transportation safety and security. Members of the Battelle Core Team (Battelle, CVSA, ATRI) recommended to the project sponsors that this would be a valuable asset to the project. The operational field testing of technology obviously requires specific technology vendors be selected as part of the test, but it was recognized that not all technology vendors and products could possibly be included in the test. Battelle selected Qualcomm, Savi, Saflink, and the Spill Center is the technology providers to serve as the platforms for this operational test. However, the real purpose of the test was to assess the potential for generic technology types to improve safety and security, not the specific products used in the test. Thus, it was considered important to identify other technologies and vendors that are available.

Outreach efforts for the Technology Compendium began with articles and news alerts directing vendors and interested parties to the *safehazmat.com* website. As of the writing of this report, the Technology Compendium includes contact information, product functionality and description, current market penetration, and pricing information for 88 different companies. Many of the original 200 technologies were identified as products that were not actually developed and were therefore not included. These 94 different companies represent 147 technologies.

Lessons Learned During Field Test

Throughout the course of this technically sophisticated field test, there were lessons learned that could be valuable for conducting similar technology tests in the future. The Battelle Team was able to witness and document these findings throughout the system installations, data collection and interaction with system users. If adjustments were feasible and did not compromise the research objectives, they were made with the advance notification of, and approval by, the project sponsor.

These lessons are documented in Section 4.6. Several of the key lessons are presented here:

- The Electronic Supply Chain Manifest (ESCM) issues typically focused around data transfer associated with slow dial-up connections and/or ISP issues. High-speed digital infrastructure such as T1 lines, DSL, and broadband cable generally eliminate ESCM connectivity issues.

- The Global Login was heavily used and some drivers preferred it to the biometric verification. Based on driver comments, the research team speculates that this finding results from some combination of (a) greater familiarity with the existing Global Login, (b) privacy concerns associated with biometric readers, and (c) more frequent technical problems with biometrics.

- Electronic seals were used in this FOT as a concept technology. While they have some utilization in other sectors of the freight industry, they are not currently used in the for-hire trucking industry. The project team found that 1) newer, heavy-duty trailers and trailer doors interfered with the tag's data transmission (the tag vendor indicated that newer versions of the tag would address this issue); and 2) even with e-seal training, it was apparent that the system was extremely complex, likely resulting in low driver usage.

- Geo-fencing as a concept had extremely high interest by both industry and government, however the technical design needs revisions including improved position resolution and more complex protocols (basis for exceptions, identification and interdiction). From a carrier perspective, this would provide better asset management.

- Although only tested in staged tests and interim visits, many drivers were extremely excited to have both the in-dash and key fob panic button. Panic buttons were viewed as "insurance policies"; carriers did not expect to use them, but felt their presence created peace-of-mind for drivers.

- For the untethered trailer tracking device, several electrical power issues arose and were centered on Pin 7 of the 7-way connector. Many trucks were found to have blown fuses. It was determined that some batteries were drained even when connected. Working with the carrier maintenance team, the issue was ultimately solved.

- Terrestrial communication systems are less expensive than satellite systems, possibly making them a preferred system for smaller carriers. One carrier conducted an internal

operational analysis of its (terrestrial) tracking system, which indicated it provided a positive ROI based on a cost-benefit survey of facility managers and data analysis.

- For the Public Sector Reporting Center concept, the various types, reliability, security, and cost-effectiveness of communications technologies as they relate to law enforcement needs to be further investigated. In addition, there is a need to investigate the issue of message priority. Battelle will conduct a Needs Assessment Task drawing on the results and findings of both the deployment team and evaluation team final reports.

- The PSRC approach, when shown to non-public sector users, was of tremendous interest to them. They saw the value to being provided with proactive messaging to enable them to enhance their safety and security programs.

1.0 Introduction

During the past two years, the Federal Motor Carrier Safety Administration (FMCSA) and the Intelligent Transportation Systems (ITS) Joint Program Office (JPO) within the U.S. Department of Transportation (U.S. DOT) has been conducting a major field operational test (FOT) to assess the potential enhancement of the safety and security of hazardous materials transportation resulting from the application of various technologies. Battelle and its team of subcontractors was selected through a competitive process by FMCSA and the ITS JPO to conduct this test. This report documents the planning, execution, and results of this major field test.

The overarching goal of the FOT was to conduct a project that would demonstrate the effectiveness of certain technological solutions (remote vehicle tracking, remote vehicle disabling, off-route alert systems, etc.) in enhancing the security of hazardous materials transportation in the commercial vehicle industry. In addition, FMCSA and the ITS JPO believe conducting this operational test will speed up the deployment of these technologies in the industry. The FOT was designed to achieve this goal by providing data to quantify the security costs and benefits of an operational concept that applies technology and improved enforcement procedures to hazmat transportation.

1.1 Background

It is important to understand the context and background leading up to the U.S. DOT taking action to procure a contract team to conduct this operational test. In the aftermath of the terrorist attacks on September 11, 2001, there was extremely heightened concern regarding the security related to the transportation of hazardous materials and the fear that terrorists might highjack a truck carrying hazardous materials or use it in some other fashion to commit a terrorist act. In addition, there was concern about possible attempts to obtain hazardous material endorsements to Commercial Driver's License (CDLs) under false pretenses. To address these concerns, Congress held a number of hearings on ways to improve the security in this field. Given that over 800,000 shipments of hazardous materials takes place each day of the year, this is a daunting challenge.

Not long after these hearings, Congress passed the PATRIOT Act that, among other things, mandated that applicants for a hazmat endorsement to their CDL must first undergo a comprehensive background check by the Department of Justice. The PATRIOT Act made note of the potential for technology to help facilitate and improve hazmat driver identification and verification.

In the meantime, FMCSA made over 32,000 contacts and security sensitive visits with hazardous materials carriers. These contacts and visits resulted in over 280 findings of "suspicious activity" and over 125 referrals to the Federal Bureau of Investigation (FBI). The FMCSA issued Security Talking Points prior to conducting these security sensitivity visits. The purpose of the security visits by FMCSA was to increase the level of awareness of motor carriers to terrorist threats and to identify weaknesses in carrier security programs. In addition to identifying specific instances of suspicious activity, FMCSA learned a great deal from the interactions with carriers and has presented its "lessons learned" for motor carries as related to

developing security plans, personnel security practices, facility security practices, and en route security practices.

FMCSA also expanded its outreach program to cover hazmat security. One example is the Security Awareness for Enforcement (SAFE) Checklist it developed in association with the International Association of Chiefs of Police (IACP). FMCSA has also developed guidelines to assist hazmat motor carriers in developing effective security plans and an extensive hazmat security training program use inspectors who will review these security plans.

Many of FMCSA's efforts are tied closely to new hazmat security planning and training regulations recently published by Research and Special Programs Administration (RSPA) that address several important areas that could improve security: (1) requiring carriers of certain hazmat to develop security plans, and (2) requiring carriers of certain hazmat to conduct driver and employee security training.

Finally, FMCSA identified an important potential role for technology to help improve motor carrier hazmat security. This was the result not only of the findings from the motor carrier security visits, but also from working with internal Department of Transportation working groups including the Intermodal Hazardous Materials Task Force and the Hazmat Direct Action Group (DAG). The internal DOT evaluation of hazmat security vulnerabilities identified a number of action items and initiatives across DOT. One major initiative was the need to take a close look at commercially available, off-the-shelf technology that could be deployed in the near term to help fill some of the most glaring gaps in hazmat transportation security.

These developments led to a competitive solicitation to field test and evaluate appropriate technology. FMCSA's intention for this field test is stated succinctly in the statement of work released to prospective bidders:

> The purpose of this initiative is to quantify the security costs and benefits of an operational concept that applies technology and improved enforcement procedures to HM transportation. A field operational test shall be conducted to demonstrate an approach that ensures the safety and security of HM shipments from origin to destination.
>
> The scope of this effort shall include activities that address the following risk areas: driver verification, off-route vehicle alerts, stolen vehicles (both tractors and trailers), unauthorized drivers, cargo tampering, and suspicious cargo deliveries. Suspicious cargo deliveries include the unauthorized shipment of certain types of HM to facilities that would not normally use the HM in their business operations and the shipment of different types of HM, that when combined, could pose a security risk.
>
> The scope of this project shall be organized in three stages: (1) the pickup of HM from shipper, (2) the transportation of the HM, and (3) the delivery of the HM to the receiver at the final destination.

FMCSA specified that the Hazardous Materials Safety and Security Operational Test (FOT) shall demonstrate an integrated operational approach that ensures the following: (1) the driver is properly identified and verified at the point of hand-off from the shipper to the carrier of the hazardous material, (2) the potential for the vehicle or trailer to be hijacked or compromised is

significantly reduced, (3) if the vehicle or trailer is hijacked, there is a prompt notification capability to cognizant authorities, and (4) the ability to quickly and efficiently respond to the threat is enhanced.

1.2 Stakeholder Involvement and Benefits

The application of technology for hazmat shipments has the potential for a significant impact on many parties involved with hazardous materials transportation. It is helpful to understand this potential impact by stakeholder group.

Shippers of Hazardous Materials – Manufacturers and shippers of hazardous materials can be targets of terrorists because of the volatile nature of their products. The obvious concern of most shippers is facility security. But the interface with carriers presents another critical activity that could allow access or intervention of terrorists for the purpose of sabotage or hijacking. Shippers of hazardous materials must comply with all the appropriate hazardous materials regulations for the preparation and certification of their shipments. Therefore, it is extremely important to shippers that the handoff of a hazmat shipment to the carrier be tightened from a security perspective. Shippers need verifiable information from the carrier that the carrier's pickup driver is the right person and he or she is picking up the correct cargo. The system tested used biometric smart card technology and electronic manifest technology that provided the shipper with driver and cargo identification and verification. The driver identification and verification system tested resulted in the clearance to release a hazmat shipment to drivers that have had background checks as a precursor to their receiving hazmat endorsements on their CDLs.

Motor Carriers of Hazardous Materials – Motor carriers will benefit the most from the technologies being tested. Motor carriers have the responsibility for the shipment once the cargo is received. By the very nature of their business, motor carriers are potentially easy targets for potential sabotage or hijacking during the movement from origin to destination. Many of the specific elements that had to be addressed in the FOT and the related technologies selected by the Battelle Team are directly applicable to intervention while en route. First and perhaps most important, was the ability to know the cargo's location through Global Positioning System (GPS) and wireless asset tracking capability and the visibility of each shipment to the dispatcher. Panic button capability and remote vehicle disabling capability were provided to drivers. The dispatchers were also provided a remote disabling capability. To address tampering with the cargo seals, the capability to send an electronic message to both the driver and the dispatcher for immediate notification to law enforcement was tested. Similarly, automatic notifications to the dispatcher were sent for unauthorized attempts to uncouple a trailer from the cab. The ability to track untethered trailers was also tested.

Receivers of Hazardous Materials – Consignees have many of the same problems as the shippers identified above. They must better manage the interface with the incoming carrier to their facilities. They must be able to identify and verify that they are receiving the shipment from the correct carrier, that the driver is who he says he is, that he has the adequate background checks, and that the cargo is correct. The same driver and cargo identification systems discussed above for the shipper provided this information to the receiver in a data-secure environment.

Public Sector Enforcement and Emergency Response – This stakeholder group is the ultimate user of alert information generated during the FOT. They must have the right amount of accurate information in order to take effective action in the event of suspected terrorist activity. Alert notification resulted from many different type of events that the implemented technology solutions could identify, including: cargo seal tampering message, a remote disabling event, carrier out-of-route notice, or unauthorized driver alert notification. Roadside enforcement will have access to driver identification and verification information.

The technology solutions tested by the Battelle Team have provided proof-of-concept for providing information to the public sector in all of these situations. In particular, we demonstrated the ability to deliver such messages to roadside enforcement, law enforcement, and emergency responders.

While the Battelle Team also included two organizations that represented the perspective of important stakeholders during the project (namely the ATRI and CVSA, the FOT included the direct participation from six shippers, nine carriers, four consignees, and six state agencies in four states. Their feedback and commitment during the project helped to ensure its overall success and ensured that their respective issues, concerns, and experiences were adequately captured and addressed.

In addition, a voluntary External Stakeholder Review Group was formed with selected members of the shipper, carrier, and enforcement communities and met periodically to review progress of the operational test and offered comments and opinions. This helped to further expand the range of represented perspectives from the very diverse hazmat industry. The Battelle Team incorporated stakeholder viewpoints into the evolving test and project reports wherever possible.

1.3 Field Operational Test Requirements

The scope of the FOT included activities that addressed risk areas such as: driver verification, off-route vehicle alerts, stolen vehicles (both tractors and trailers), unauthorized drivers, cargo tampering, and suspicious cargo deliveries. The FOT was divided into eight separate tasks and organized in three stages: (1) the pick up of hazardous materials from the shipper, (2) the transportation of hazmat, and (3) the delivery of hazmat to the receiver at the final destination and was centered around 23 separate research objectives. These research objectives are discussed in detail later in Section 3.0 of this report.

The FOT was conducted over a 24-month period. The initial eight months were focused on program planning and development activities, followed by a brief pilot test period and then the field deployment and data collection activities. The pilot test period entailed a final design review meeting where the final system designs for all technology components were presented to FMCSA and the ITS JPO for review and approval. See Table 1 for FOT requirements.

Table 1. FOT Requirements

Task		Description
1	Risk and Threat Assessment	High-level analysis of the safety and security risks and threats; used to frame the Concept of Operations
2	Concept of Operations	Detailed narrative of the proposed test; matched up the identified risks and threats with the required test elements
3	Develop Requirements	Included a detailed operational requirements analysis and mapped the results to requirements and specifications
4	Develop System Design	Included logical and technical architectures, subsystem design, and interface design
5	Conduct the Field Operational Test	Prototype demo followed by the six-month full test including installation, operation, and data collection
6	Evaluation	Supported the independent evaluator in the evaluation of test plans, data collection, and data analysis
7	Final Project Report	This document, which summarizes the lessons learned and the results of the FOT
8	Final Evaluation Report	Supported the independent evaluator in the development of the final evaluation report

Once the design was approved, final system integration activities were completed and a full-scale pilot test of the technologies was conducted. The pilot test was designed to test each of the proposed technology applications on-board a commercial vehicle, as well as collect sample data and "exercise" the data collection, filtering, and delivery process from the deployment team to the evaluation team. The pilot test was conducted in late-summer 2003 and was conducted at Qualcomm's San Diego, California facilities. In order to minimize the impact to our volunteer carrier participants, the technologies were installed and integrated into the Qualcomm Technology Truck for the pilot test. The technologies were integrated so that each component could be activated or disabled as needed so the exact configurations of each scenario could be simulated.

The deployment team worked with the evaluation team to establish the specific data elements to be collected, how this information would be stored and forwarded to the evaluation team. This process was exercised during the pilot test period and proved to be a significant benefit to the eventual smooth operation of the full deployment test and data collection.

Once the pilot test and sample data collection activities were completed, FOT activities shifted to full-scale deployment and operation of the operational test. Installations began in late August, 2003 and the operational period completed in early May, 2004.

The FOT deployment team (see Section 1.5) was required to include (at a minimum) four motor carriers, 100 tractor-trailer units, four shippers, four receivers, a systems integrator, and hazmat industry and state safety enforcement representatives. Based on recommendations from the deployment team and the successful pilot test, FMCSA and the ITS JPO agreed to shorten the field-testing period from the original ten month requirement to six months. This

recommendation was made in order to minimize the time-burden on the carriers, shippers, and consignees associated with their participation in the FOT and to encourage consistent involvement throughout the testing period by these organizations. As discussed later, this proved to be a critical success factor in the overall continuity and success of the FOT.

FMCSA also identified a need to conduct a strategic assessment of the needs and requirements of the emergency responder and law enforcement communities. As a result, a Public Sector Needs Assessment task was added to the eight requirements listed above. This needs assessment will be completed after both this document and the final evaluation report are accepted by FMCSA and will, therefore, be prepared as a separate document. It will take into account the technical aspects of the FOT as well as the technical results from the independent evaluator to develop the strategic recommendations to DOT to address public sector needs and requirements. The needs assessment will entail:

- Convening meetings of team participants and appropriate FMCSA and FHWA representatives to discuss critical issues.
- Conducting a major stakeholder workshop with key stakeholder throughout the emergency responder community.
- Documenting the lessons learned during the conduct of the FOT.
- Developing a strategic assessment and recommendations for DOT to address the critical issues.

1.4 Description and Organization of this Document

This document covers the work completed by Battelle and its subcontractors as part of the deployment activities for the FOT. The purpose of this final report is to document the activities of the Battelle Team, how we assembled the technology providers to address the research objectives, and the results and issues that arose from field testing the technologies. We will not attempt to duplicate the detailed material provided in task reports delivered earlier in the program (e.g., Risk/Threat Assessment, Concept of Operations). Rather, where appropriate, we will direct the reader to the specific documentation for more detailed information.

Because many of the documents produced from earlier activities contained material that was considered "sensitive" and its release needed to be controlled, some documents and results have been categorized as Sensitive Security Information (SSI) by the U.S. DOT. Disclosure and release of SSI is controlled by the U.S. DOT and is restricted to authorized people on a need-to-know basis. In addition, since one of the underlying principals in designing the FOT was to use current off-the-shelf (COTS) systems and technologies wherever possible, some of the specific architecture, design, and operational characteristics of the technology components are considered business sensitive by FOT team members. All SSI and business-sensitive material will be included in Appendix E. See Table 2 for organization of FOT final report.

Table 2. Organization of FOT Final Report

Chapter		Description
1	Introduction	Background, requirements, organization, and development of the project team
2	Hazardous Materials Transportation	Industry overview, analysis, compendium of technology providers; security concerns
3	Research Objectives and Approach	Objectives and how the approach for the FOT was developed
4	Methodology and Conduct of the Field Operational Test	Details the specific approach to addressing each of the functional requirements; the technologies and methods deployed; includes the threat and vulnerability analysis, development of scenarios and technology suites, the conduct of the FOT, and lessons learned
5	Findings and Next Steps	Includes findings and recommended next steps

1.5 Project Team

Battelle assembled a team of technology developers and vendors, hazmat industry shippers and carriers, and security experts that worked together to demonstrate the feasibility of the 23 research objectives defined by FMCSA. Table 3 provides a snapshot of the team and each member's role as an aid to the following discussion.

Battelle served as the prime contractor, system integrator, program manager, and hazmat transportation domain expert for this project. Battelle has a long history providing technical support since the 1950s to DOT, Department of Energy and Department of Defense in hazmat and nuclear transportation.

Battelle assembled and led a "core team" of partners to address FMCSA's requirements. This core team included Qualcomm, the American Transportation Research Institute (ATRI, formerly the American Trucking Association Research Foundation), and the Commercial Vehicle Safety Alliance (CVSA). The core team served as a central project planning group that set direction and responded to problems and issues as the project unfolded.

Qualcomm is the single largest provider of technology solutions to the motor carrier industry. Their system served as the wireless communication backbone of the Battelle Team's overall technical approach. Qualcomm served as the technical lead organization and was responsible for ensuring the interface of its system with other technology providers on the team.

ATRI was a member of the core team for two reasons. ATRI represents the interests and experience of the critical industry group to ensure success of this project – the motor carrier industry. Second, its staff had substantial and current experience in managing field operational tests demonstrating new technology to improve security in supply chain management.

CVSA was the final member of the Battelle Team because of their unique role in representing the perspective and interests of the "public sector" side of this project – state enforcement and response agencies. This was a critical perspective that had to be an element of all phases of

project planning and performance. CVSA is a non-profit organization of federal, state, and provincial government agencies and representatives from private industry in the United States, Canada, and Mexico dedicated to improving commercial vehicle safety.

Table 3. Battelle Team Members

Core Team Planning Group	
Battelle	Prime Contractor; System Integrator; Hazmat Domain Experts; Risk Assessment; Evaluation Coordinator
Qualcomm, Inc.	Primary Technical Lead; System Development
American Transportation Research Institute (ATRI)	Industry Liaison; Electronic Supply Chain System; System Development Support; Support Evaluation Coordination
Commercial Vehicle Safety Alliance (CVSA)	Public Sector Liaison; Coordinate State Enforcement and Responder Involvement; Assess Needs of Public Sector
Total Security Services International, Inc. (TSSI)	Trucking Security Experience; Threat Assessment Task
Technology Providers	
Qualcomm, Inc.	Technology Integrator System Development; Provide Technology Products to Address Functional Requirements with Interfaces to Other Technology Partners
Saflink Corporation	Biometric Smart Card Provider; Driver Verification and Cargo Tracking System (ESCM)
Savi Technology, Inc.	Radio Frequency Identification Tags and System Provider; Cargo Tampering Tasks
The Spill Center	Hazardous Materials Support and Environmental Claims Management Company

As identified in Table 3, the other team members include technology providers who worked closely with the core team in providing their own technology solutions to demonstrate functionality of specific functional requirements.

- **Saflink** had a critical technical role to play on the team by providing the biometric smart card capability to demonstrate driver identification and verification functionality. In addition, Saflink provided the electronic supply chain application that was integrated with other project team technologies to demonstrate driver verification throughout the pickup, en route, and delivery cycle of a hazmat shipment.

- **Savi Technology, Inc.**, provided its Radio Frequency Identification Device (RFID) and electronic logistics solutions capabilities that were integrated with the project team technologies to demonstrate electronic cargo seal integrity.

- **The Spill Center**, a leading hazardous materials support and environmental claims management company, integrated their reporting system technology to provide the backbone for the public sector reporting center (PSRC).

- **Total Security Services International, Inc.** (TSSI) was added to the team to provide technical leadership in conducting the threat assessment during Task 1. TSSI is a preeminent trucking security consultant supporting the American Trucking Associations and addressing motor carrier industry security threats since the September 11, 2001 tragedy.

2.0 Hazardous Materials Transportation

2.1 Industry Profile

2.1.1 Industry Dynamics

The trucking industry is a very large and complex sector of the U.S. economy. The largest sector of the freight industry in both tonnage and freight revenue, the trucking industry utilizes a wide variety of vehicle configurations to move nearly ten billion tons of goods every year, representing almost 70 percent of all domestic shipments.

The recent upswing in both the domestic and international economies is likely to increase the size and complexity of the industry. Past market forces that impacted the trucking industry included just-in-time deliveries and deregulation. Developing influences include increasing competition, driver shortages, security concerns, an expanding regulatory environment, and growing technology investments. In total, these effects are changing the way the trucking industry moves goods.

The hazardous materials transportation sector of the trucking industry is experiencing similar changes and impacts. Hazardous materials themselves are constantly changing and evolving along with the federal programs that govern them. It is clear that hazmat shipments are growing in synchronization with overall freight growth, although hazmat shipment data are difficult to access and analyze. One minor exception to this trend is that was a slight increase in small package hazmat shipments in 2002 (1 to 1.5 percent) while there was a similar decrease in the number of overall small package freight shipments.[2]

2.1.2 Sector and Commodity Growth

RSPA estimates that daily hazmat shipments exceed 800,000, resulting in 300 million annual shipments.[3] Again, it is difficult to collect specific data on hazmat since it is a secondary category, rather than a specific commodity description, and most data sources do not provide data at the commodity level. It is known that services and manufactured commodities associated with hazmat shipments are growing. For instance, over the next five years it is estimated that the following industry sectors will experience healthy growth (Table 4).

It is intuitive that requisite growth will occur in the hazmat components used in these sectors.

Overall, government forecasts put hazmat tonnage growth at approximately two percent per year.[4] In a growth economy, this would quickly result in a dramatic increase in hazmat capacity demand within the trucking industry.

---

[2] U.S. Freight Transportation Forecast…To 2014, American Trucking Associations, 2003. p. 22
[3] Office of Hazardous Materials Safety U.S. Department of Transportation. Hazardous Materials Shipments. Washington, D.C., Oct 1998. Available at hazmat.dot.gov.
[4] Department-wide Program Evaluation of the Hazardous Materials Transportation Programs, Executive Summary, March 2000, p. 17. Available at http://hazmat.dot.gov/hmpe_report.pdf.

Table 4. Estimated Annual Growth Rate by Industry Sector[5]

Industry Sector	Average Annual Growth Rate 2003 – 2008
Paper and Products	2.6%
Printing and Publishing	2.2%
Chemicals and Products	4.0%
Rubber and Plastics	2.8%
Fabricated Metal Products	2.5%
Electronic Components	7 to 14%

2.2 Hazmat Industry Technology Analysis

2.2.1 Objective

The FOT was focused on a limited number of participants; approximately nine trucking companies and 100 vehicles. In an effort to determine how representative the FOT findings are to the hazmat industry as well as increase the reliability and validity of the FOT, the Battelle Team gathered comprehensive data on the hazmat trucking industry.

2.2.2 Methodology

The data collection approach was developed with significant input from the Battelle Team, FMCSA, and the Independent Evaluation Team. Data for a small group of representative hazmat carriers were gathered to test the effectiveness of the proposed approach. Based on the results of that effort, revisions were made and the larger effort was undertaken. Ultimately, data on 164 hazmat carriers were obtained. These carriers were culled from several different carrier information databases such as the National Fleet Directory, intrastate databases, and the National Tank Truck Carriers membership.

2.2.3 General Findings

The data gathered focused on several different types of information such as:

- Respondent demographics, e.g., fleet size, range of operation, carrier type
- Routing and other operational issues
- Hazmat commodities hauled
- Security concerns and issues

[5] U.S. Freight Transportation Forecast to 2015; American Trucking Association, Inc., 2003.

- Current and future technology use

The following are highlights from each of these areas.

Respondent Demographics

The analysis tool collected data on the number of power units operated by their company. These were categorized using FMCSA-designated categories (Table 5).

Table 5. Industry Characteristics by Number of Units Operated

Category	Number of Units	Percentage		
		FOT Industry Analysis	MCMIS Hazmat Carriers	CVO Industry*
Very Small	6 or less	8.5	38.4	87.4
Small	7 to 20	18.8	27.8	8.5
Medium	21 to 100	38.8	24.3	3.4
Large	100 or more	29.7	6.6	0.7
Unknown		4.2		

*FMCSA database August '03

Thirty percent of hazmat carriers operate more than 20 power units, according to the Motor Carrier Management Information System. This differs from the industry as a whole in which only four percent fall into this category, possibly indicating that there is a preponderance of larger carriers in the HM sector. This was also found to be the case in the FOT Industry Analysis, in which the majority of the respondents (68.5%), reported operating more than 20 power units.

Respondent Range of Operation and Hazmat Material Transported

The range of operation and type of hazmat hauled for each carrier were determined. The average length of haul was stratified using categories from the 1997 Vehicle Inventory and Use Survey (VIUS) produced by the U.S. Census Bureau [1]. The VIUS is a sample survey of private and commercial trucks registered (or licensed) in the United States as of July 1 of the survey year. It is used to measure the physical and operational characteristics of the U.S. truck population. Table 6 explores range of operation for the FOT Industry Analysis, VIUS Hazmat Carriers, and the general CVO Industry as derived from an August 2003 FMCSA database query.

For comparison purposes the percentages are compared with other data on the hazmat and general CVO industries. As can be seen it was easier to obtain data for the longer-range carriers.

Hazmat transporters move a wide variety of hazmat commodities. Figures 1 and 2 present a distribution for which the companies haul particular hazardous materials (based on classifications). In analyzing numerous breakdowns of HM shipped, flammable liquid represents

the largest percentage of HM cargo by volume. This finding is congruent with data from the Commodity Flow Survey which reports that 80.8 percent of total hazardous material tonnage is Class 3 flammable liquids.[6]

Table 6. Hazmat Carriers Range of Operation

Category	Number of Miles	Percentage		
		FOT Industry Analysis	VIUS Hazmat Carriers	CVO Industry*
Local	Less than 50	15.8	30.7	39.5
Short range	51 to 100	18.2	19.0	16.7
Short-range medium	101 to 200	21.2	10.9	10.8
Long-range medium	201 to 500	28.5	17.4	12.2
Long range	More than 501	8.5	19.5	16.0
Unknown		7.9		

*These numbers derived from an August 2003 FMCSA database query.

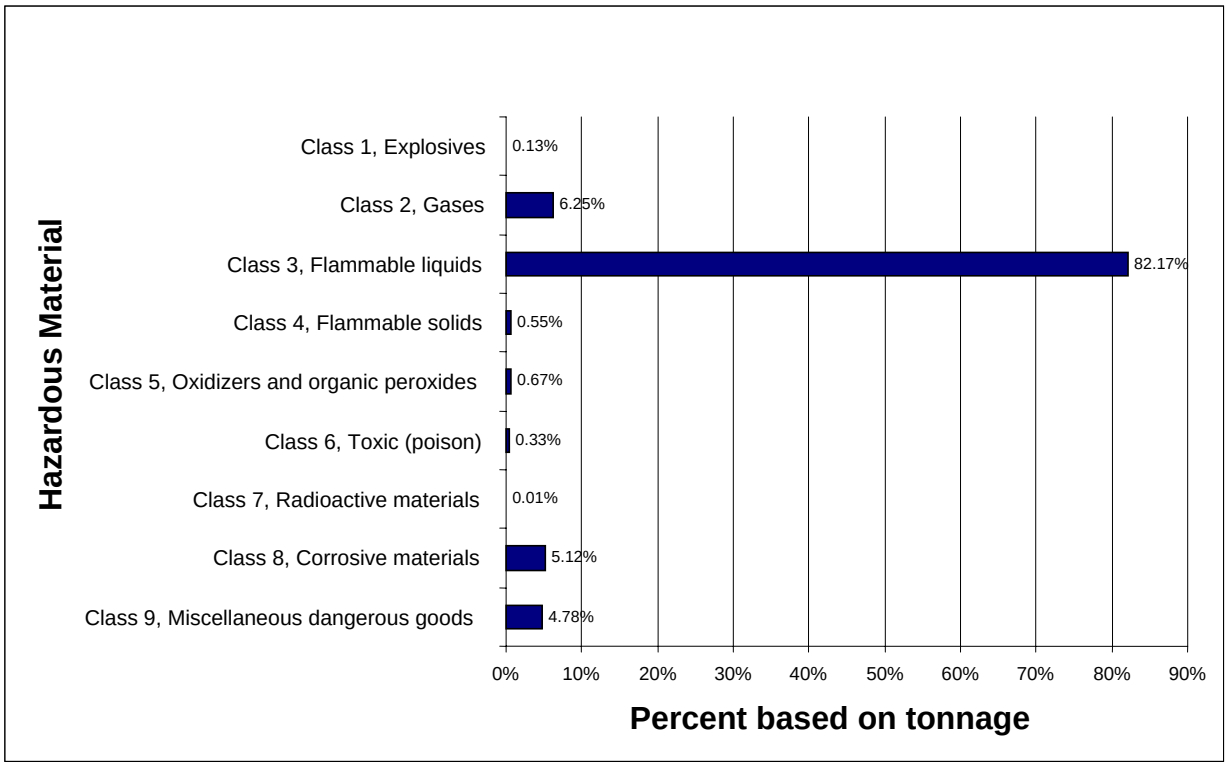

Figure 1. Hazmat Transported/CFS 1997

[6] Commodity Flow Survey, Hazardous Materials, 1997.

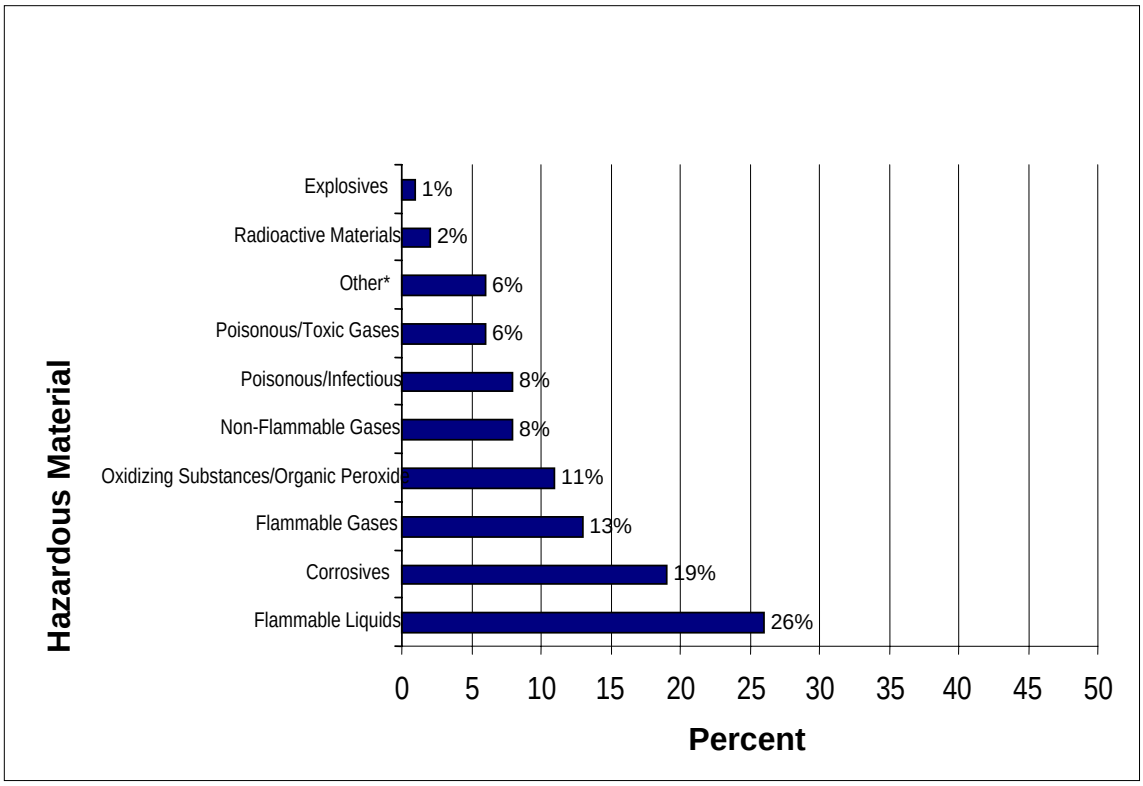

Figure 2. Hazardous Material Transported by Company (FOT Participants)

More than 80 percent of total hazardous material tonnage by all modes is Class 3, flammable liquids. Specifically, 82.2 percent of Class 3 hazmat is transported by trucks.

Security Concerns and Issues

The number and variety of security concerns and issues have multiplied for trucking companies since the tragic events of September 11, 2001. With new security legislation, trucking companies are faced with myriad issues that must be accounted for to ensure safe, compliant transport of commodities. The five leading security concerns and/or issues relating to hazardous materials transport were identified for many of the companies.

The top three issues as identified by the FOT Industry Analysis were as follows:

1. En route security
2. Cargo theft
3. Sabotage and tampering

Prior to 9/11, cargo theft was the number one issue based on previous surveys and continues to be a critical concern. Vehicle theft was also identified as one of the top security concerns; when "vehicle security" is included with "vehicle theft," the category moves into the top three issues

and concerns. Not listed as a separate issue but often cited as a solution to vehicle theft/security is "secured parking facilities." Cargo security, traffic congestion, and awareness of security concerns were among others identified. It is quite evident that the trucking industry, and hazmat transporters in particular, have a large number of security concerns.

Current and Future Technology Use

Another objective of the effort was to determine which technologies are in use today, and which technologies carriers are likely to purchase in the future. For the purposes of this analysis, "future" was defined as the next two to three years. Vendors were identified, where possible, for each technology used. Figure 3 captures the current and future use of these technologies. The "current" use of each technology describes number of companies that indicated they presently use a specific technology. "Future" use is a cumulative percentage of those currently using a technology (assuming they will continue to do so in the near future defined as two to three year time frame) and those companies that indicated they presently do not utilize a technology but plan to invest in it within two to three years.

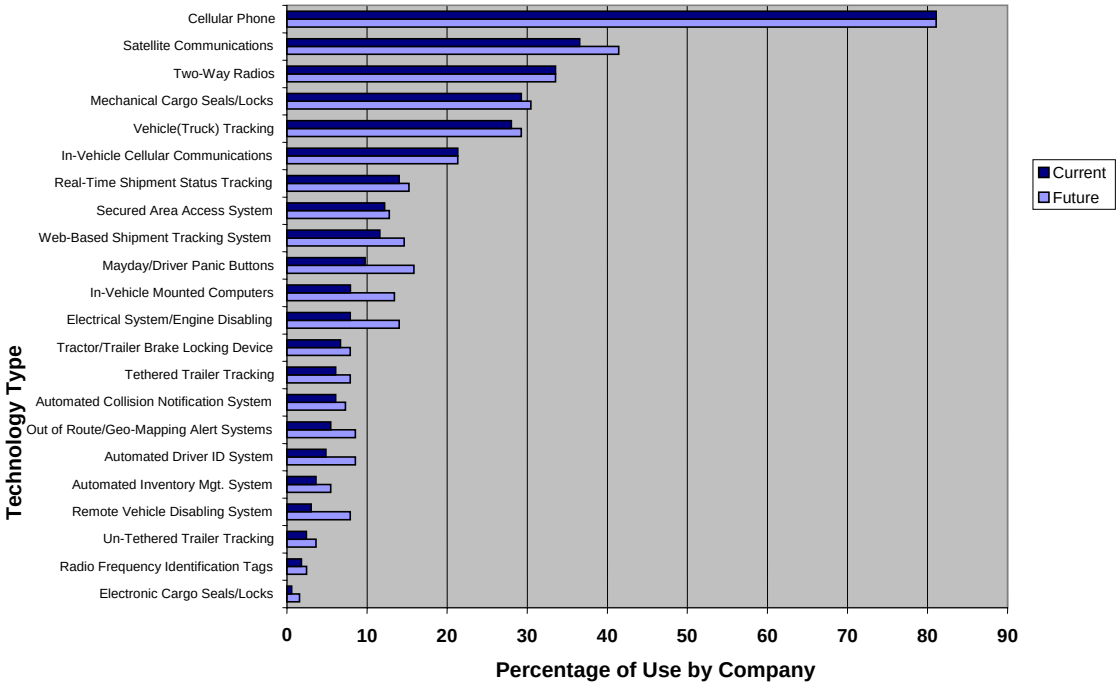

Figure 3. Current and Future Technology Use

2.3 Technology Compendium

2.3.1 Objective

The Technology Compendium, an important component of the FOT, is a compilation of trucking industry technologies currently in the marketplace. Many of these technologies have the ability to fulfill a functional requirement or act as a surrogate for technologies tested in the FOT. As a stand-alone section of the final FOT report, the technology compendium will serve as an important resource for the trucking industry.

2.3.2 Methodology

Outreach efforts for the Technology Compendium began with articles and news alerts directing vendors and interested parties to the safehazmat.com website. The "safehazmat.com" website was built to provide the general public with information on the FOT and its technologies, team members, and as a portal for interested technology vendors to submit general information on their product for inclusion in the technology compendium. Internet searches were performed for additional technologies. A number of the vendor companies were contacted via phone, and approximately 35 to 40 in-depth interviews were performed to garner more detailed product information. For those companies that did not respond to telephone messages, initial e-mails and faxes, e-mails were sent out with their segment of the compendium spreadsheet to confirm information accuracy.

In addition, there was strong interest from technology vendors that had seen presentations on the FOT at various events and conferences. Lastly, interviews were conducted at trucking industry events such as the 2003 American Trucking Associations Management Conference and Exhibition.

2.3.3 Results

The Technology Compendium, currently formatted in a Microsoft Excel spreadsheet, originally had nearly 200 registered technologies. Based on interviews and system analyses, the Technology Compendium was culled down to contact information, product functionality and description, current market penetration, and pricing information for 94 different companies. Many of the original 200 technologies were identified as products that were not actually developed and were therefore not included. These 94 different companies represent 147 technologies. The research team collected pricing information for approximately 35 percent of the represented systems. A portion of the companies did not feel comfortable or were not able to share pricing for their products. Others did not respond to any of the outreach efforts.

2.3.4 Technologies

The Technology Compendium can be stratified and viewed in a number of ways. To increase direct relevance to the FOT, the research team developed a first-level category based on function. Consequently, the Technology Compendium can be analyzed as follows:

- Biometrics – Biometric systems represent 12 percent of compendium technologies. These are primarily biometric fingerprint readers that have the ability to integrate with a variety of security access and ID applications.

- Software – Software systems represent 18 percent of compendium technologies. The products provide integration capabilities and a variety of value added services such as mapping and operational efficiency metrics.

- Asset Tracking – The compendium includes 14 percent asset tracking systems. Many of these systems can be used for tethered and un-tethered trailer tracking.

- Cargo Seals – Cargo seals comprise four percent of the compendium. These seals range from sophisticated wireless GPS to adhesive seals. They also represent both disposable and reusable "e-seal".

- Locks – Eight percent of the compendium is composed of locks. These locks ranged from a king-pin lock to more sophisticated internal trailer door locks which require a wireless command to open.

- Anti-hijacking/Security – The compendium includes one system that provides a covert suite of security devices for managing trucks, including biometrics, pressure sensors, and vehicle disablement. Together they make up one percent of the compendium.

- Vehicle Tracking – The compendium separated asset tracking from vehicle tracking for functional purposes. The Technology Compendium includes 41 percent vehicle tracking systems. These systems include satellite, terrestrial, or hybrid systems. Many of them are based on, or incorporated, GPS.

- Employee Emergency Monitor – The compendium includes one product that allows a worker to send a distress signal if they are hurt or incapacitated.

- Asset Securement – The compendium includes one system that provides an automated explosion suppressant foam used primarily in tanker trucks.

See Figure 4 for percentages of compendium technologies.

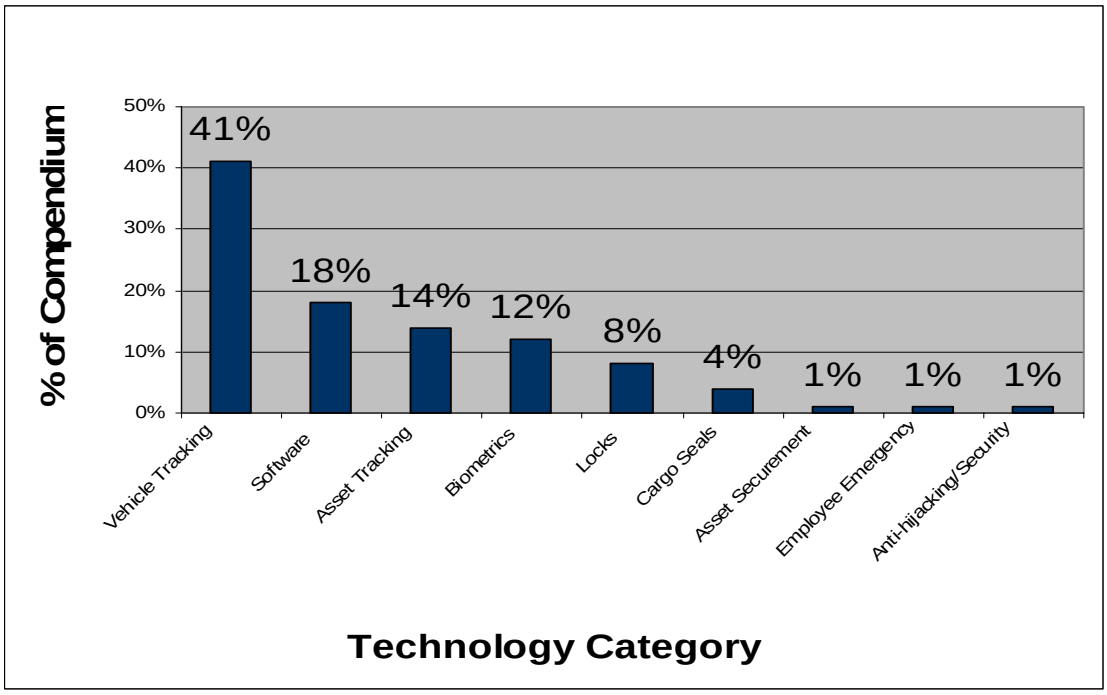

Figure 4. Compendium Technologies

The technology compendium proved to be an important part of the FOT. For those technology vendors who wished to be a part of the FOT, the technology compendium provided an avenue for them to participate in an alternate manner. It also provided valuable information on functionality, pricing, and market penetration for security technologies. The level of data found in the technology compendium has yielded extremely useful findings for the FOT. Additional findings on the technology compendium can be found in Appendix C.

3.0 Research Objectives and Approach

The scope of this FOT was centered on activities that address the following risk areas:

- Driver verification
- Off-route vehicle alerts
- Stolen vehicles (both tractors and trailers)
- Unauthorized drivers
- Cargo tampering
- Suspicious cargo deliveries

The FOT was engineered to demonstrate an integrated operational approach that made use of COTS technologies and addressed as many of the prescribed research objectives as practicable. The following discussion documents these research objectives and identifies the technology applications deployed by the Battelle Team to address them.

3.1 Prescribed Research Objectives

Each of the risk areas identified above were further organized into the three phases of hazmat transportation: (1) the pickup of hazmat from shippers, (2) transportation of hazmat, and (3) the delivery of hazmat to the receiver at the final destination. In addition, the specific objectives that related to the public sector cut across each of these phases. The relationship between these phases and the public sector are outlined in Figure 5 along with the specific objectives the FOT was required to address.

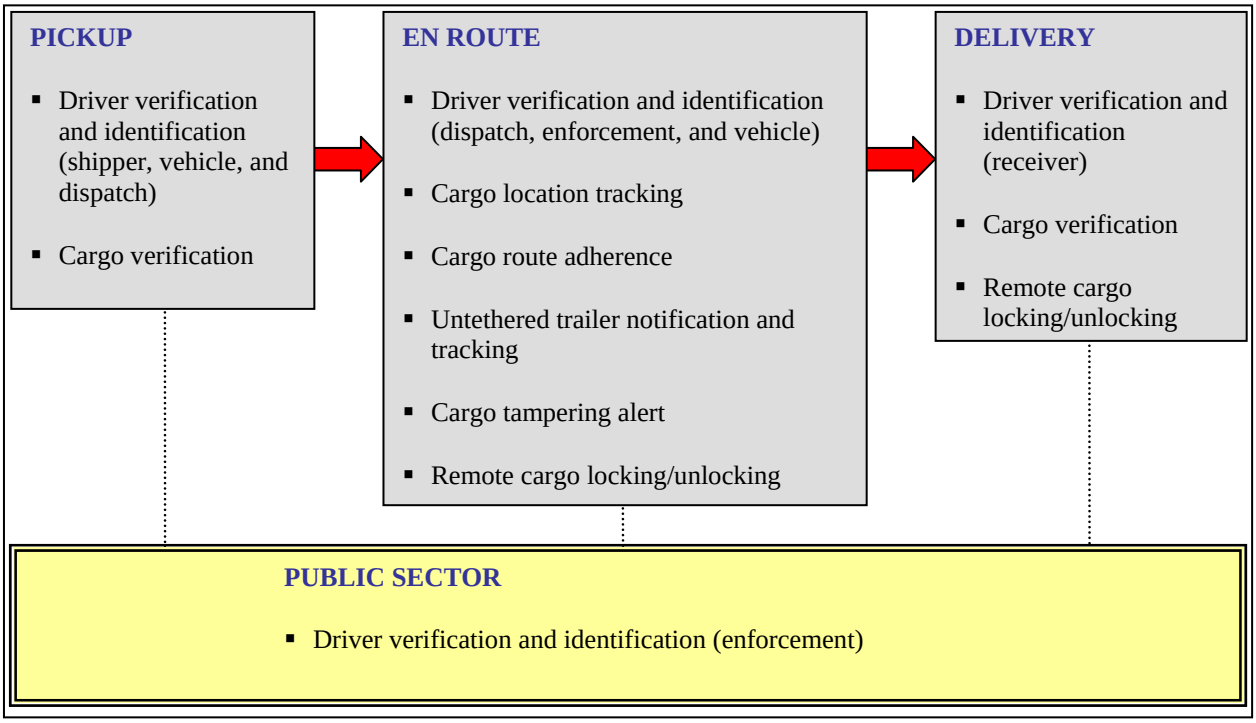

Figure 5. Prescribed Research Objectives

3.2 Adaptation of the Research Objectives to the Field Operational Test

As an important first step in FOT, a risk/threat assessment (Task 1) was conducted to organize the safety and security risks and threats in the highway transportation of hazardous materials [2].

3.2.1 Threats and Vulnerabilities

The Battelle Team adopted a multi-step approach to conduct the threat and vulnerability analysis.

Figure 6 illustrates the assessment process developed to conduct this task. The assessment began with a look at the broad universe of hazmat transportation. This universe is extremely varied, encompassing a diverse set of factors that need to be considered in conducting a risk/threat assessment, including:

- Type and characteristics of commodity
- Quantity of hazmat in individual shipments
- Frequency of hazmat shipments
- Type of operation (e.g., bulk and non-bulk, private and for-hire)
- Routing and length of haul
- Commodity loading and transfer points

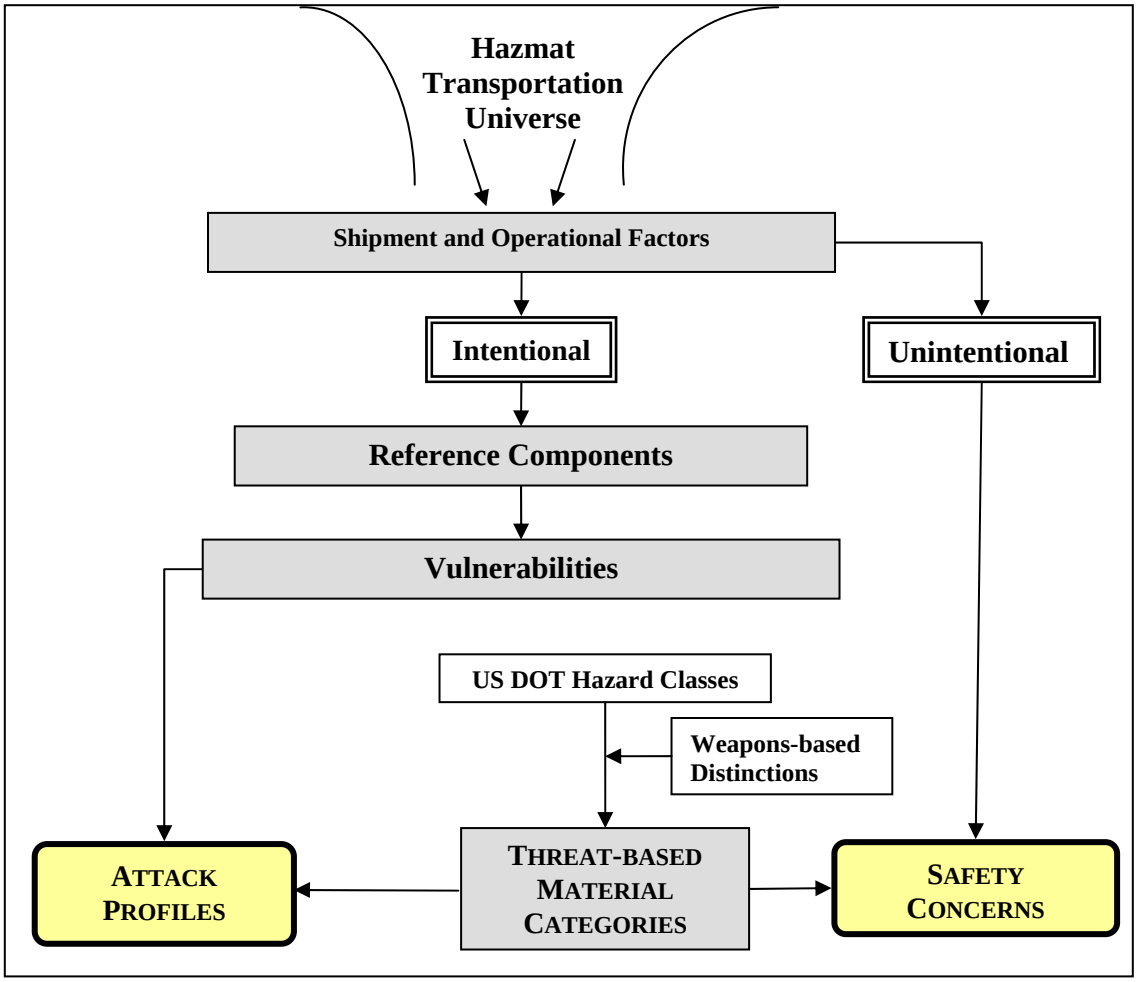

Figure 6. Process Flow

These factors were then considered from two very different perspectives: intentional vs. unintentional releases. Because the scope of work for the FOT included consideration of both security and safety, both intentional (i.e., terrorist threat) and unintentional (i.e., accidents and incidents) releases were addressed. As shown in Figure 6, a greater portion of this effort was focused on terrorist-based intentional releases, but safety-related unintentional releases were considered as well. This emphasis on security issues stems from the significant effort in the past to understand and address the safety implications of hazmat transportation; it is only recently that specific attention has been directed toward security issues.

Reference Components

To address intentional releases, general categorizations for shippers, carriers, consignees, and en route conditions were defined. The definitions for specific reference components included typical operations and characteristics. Carrier and en route conditions were grouped together. The reference components used were:

Shipper: Warehouse/reseller, hazmat manufacturer, academic/research facility, and hazmat waste generator

Consignee: Residential consumer, warehouse/reseller, industrial consumer, construction or mining consumer, academic/research facility, and waste disposal facility

En Route: Rural Interstate, urban Interstate, rural arterial or two-lane highway, urban arterial, truck stop, rest stop or parking area, weigh station and border crossing, carrier terminal, and transfer terminal

The primary purpose for defining reference components was to organize, identify, and represent typical vulnerabilities. Each reference component was defined not to represent industry best practices related to security but to reflect the combination of vulnerabilities that can be readily found throughout industry. A reference component cannot be deemed typical in aggregate, but individual characteristics are taken from typical cases. The reference components were developed from industry knowledge and were confirmed and augmented by visiting facilities and/or conducting interviews with persons responsible for the transportation of hazmat.

As Figure 6 shows, the next step in the assessment process was to identify vulnerabilities for each reference component. The vulnerabilities were then categorized according to physical security, information integrity, operations, or environment. The specific vulnerabilities highlighted for each reference component are listed in Table E-1 in Appendix E.

Attack Profiles and Safety Concerns

The Battelle Team also identified terrorist tactics that would be effective against hazmat transportation. These tactics are also called attack profiles. In the FOT, a comprehensive database of threats developed by a member of the Battelle Team, Total Security Services International, Inc. (TSSI), was examined for those threats relevant to the transportation of hazmat and specifically to the vulnerabilities identified for the reference components. Three key threats were identified: theft, interception (including diversion), and legal exploitation. For simplicity,

diversion is considered a special case of interception and these two were combined and treated as a single threat. A simple definition of these threats follows.

Theft – to take control by stealth, deception, or force

Interception – to release, detonate, or ignite while at or near a target

Legal exploitation – to exploit the system in a "legal" way so as not to arouse suspicion, for example, to acquire hazmat by commercial transaction or diversion using "insiders"

In addition, the two major types of transportation operations, bulk/truckload and less-than-truckload (LTL) shipments were considered in developing attack profiles. The three threat types were then applied against each of the two operational types to develop six different attack profiles that address the intentional use of hazmat as a weapon.

Safety concerns were also addressed at this stage by consideration of unintentional releases from accidents or incidents. Considerable prior work has addressed this issue from a purely risk perspective and the results from the most recent study for the FMCSA were included [3].

The attack profiles were then considered for different types of hazardous materials. The DOT hazard classifications were reviewed from a "weapons-based" perspective and new threat-based material categories were developed. When considering the use of hazmat as a weapon, additional distinctions are made between materials in the same U.S. DOT hazard class. For example, most gases with a toxic-by-inhalation (TIH) hazard are in a single U.S. DOT hazard class[7]. These TIH gases include those that are heavier than air (HTA) and those that are lighter than air (LTA). To a terrorist, these materials are distinctly different in their weapons potential and in how they would be used against a target (i.e., the tactics that would be used and even in which targets might be more appropriate). An HTA TIH gas might be more easily directed from a cargo tank on the surface into an enclosed underground area such as a subway station; whereas, an LTA TIH gas might be more easily spread throughout a multi-story building when released at ground level. In addition, if notification was received that a TIH shipment was unaccounted for (through the Highway Watch Information Sharing and Analysis Center, for example), a slightly different response could be initiated depending on whether the material was HTA or LTA. From these considerations, a slightly revised categorization of hazmat was developed that considered weapons-based distinctions (see Table E-2 in Appendix E). Additional discussion about these material categories can be found in the Task 1 report [2].

Table E-8 in Appendix E shows the prioritization of the six threat-based attack profiles as well as the two that are accident-based.

[7] Not all TIH materials are gases; some liquids are also TIH materials, depending on their volatility and the concentrations at which they can cause serious injury or death.

3.2.2 Scenario Development

A critical component in developing the Concept of Operations (ConOps) was the detailed definition of the four operating scenarios (Table 7). These eight attack profiles were then mapped against the four scenarios developed as part of the Battelle Team's initial planning efforts. This was done to determine if all of the attack profiles were addressed in the proposed approach.

Table 7. Proposed Scenario Descriptions

Scenario	Material	General Description
Bulk Fuel Flammable Gases/Liquids	Class 3, Flammable Liquids	Short-haul fuel delivery vehicles
LTL High Hazard	Class 3, Flammable Liquid Class 6.1 Poison Class 8 Corrosive	LTL and dray chemical vehicles
Bulk Other TIH	Class 2.2 Non-Flammable with Inhalation Class 3 Flammable Class 9.2, 4, D Ester	Bulk chemical vehicles
Truckload Explosives	Class 1.1 – 1.6	Explosive or radioactive materials vehicles

The next step was to determine if the four proposed scenarios covered the various components (shipper, route, and consignee) of the hazardous materials movement process defined in the threat and vulnerability assessment [2]. Because many of the scenarios were divided into sub-scenarios, the field test was able to cover more of the various components than it would have otherwise. Refer to Appendix A for a detailed description of each scenario and the specific shipper, route, and consignee elements that each contains. Based on the results of this mapping exercise, it was determined that the four proposed scenarios sufficiently covered the various components of the hazardous materials movement process listed above in Table 7.

The next step was to focus on evaluating the vulnerabilities identified in the threat and vulnerability assessment and determine which technologies would be tested in each specific scenario.

First, each proposed technology component was evaluated against the vulnerabilities to determine which technologies could address specific vulnerabilities. While there were over 30 specific vulnerabilities identified, some could not be addressed by technology solutions. The vulnerabilities were separated into four categories: operational, environmental, physical, and information integrity. Operational vulnerabilities (e.g., lack of delivery notification, limited driver verification) were those that could be addressed through changes and/or modifications to operational procedures. Many of these lent themselves to the application of technology solutions to reduce the vulnerability and increase security. Environmental vulnerabilities (e.g., high population nearby, traffic congestion) were those associated with the general environment surrounding the hazardous materials shipment. Typically, technology solutions will not have an

impact on these vulnerabilities. Physical vulnerabilities (e.g., unsecured perimeter) typically represent a security concern that is associated with the physical surroundings and security. Many of these vulnerabilities can be addressed, but were out of the scope of the FOT. Finally, information security vulnerabilities represent concerns with the electronic security, access, and validity of data. Again, there are technology solutions that can be applied to these areas to improve their security, but this area was also outside the scope of this FOT.

Once the technologies were identified that could address the specific vulnerabilities within the scope of the FOT, it was necessary to evaluate the proposed solutions against FMCSA's research objectives. Table E-10 in Appendix E shows the relationship between the scenarios, vulnerabilities, and research objectives. As a result of this mapping, two of the research objectives originally specified by FMCSA were not supported by the vulnerabilities identified in the threat and vulnerability assessment. These two functional requirements were:

- Real-time emergency alert message notification by the vehicle after the vehicle is involved in a crash
- Auditable log of all shipments to be kept by the motor carrier

3.3 Technologies Addressing the Research Objectives

Selection of the technologies was focused around addressing the research objectives associated with the pick-up, en route, and delivery functions as well as addressing the vulnerabilities identified in the threat and vulnerability analysis. A description of each technology component is included later in Section 4.4.2 of this report. Table 8 presents a mapping of the FOT research objectives against the technologies selected for the test. A detailed description of how each functional requirement was addressed (technologies deployed, shippers, carriers, consignees, and outcome of the testing) is discussed later in Section 4.4.

There is only limited empirical research available on the impact of technology on user behavior, particularly truck drivers. Several studies are now underway to ascertain the effects of on-board technology usage and affects – particularly from a driver distraction perspective. Anecdotally, it is assumed that, as more and more "telematics" technologies are incorporated in a truck, the potential impact on safety and efficiency increases.

Outside of truck drivers, most economic studies support the use of technology as a productivity tool. From a behavioral perspective, the effects are not well understood.

Table 8. Mapping Research Objectives to FOT Technologies

	Research Objectives	Comm. (Satellite Terrestrial or Digital Ph)	Global Login	Biometric Verification	In-Dash Panic	Wireless Panic	On-Board Computer	Electronic Manifest	Electronic Seals	Geofencing	Untethered Trailer Track	Cargo Trailer Locking	Tethered Trailer Track	Remote Disabling	PSRC
1.1	Hazmat driver identification and verification by the shipper	S	✓	✓											
1.2	Hazmat cargo verification by the driver, dispatcher, and receiver	S,T						✓							
1.3	Hazmat driver identification and verification by the vehicle	S	✓	✓											
1.4	Hazmat driver identification and verification by the dispatcher	S	✓	✓											
1.5	Hazmat cargo tampering alert to the driver and the dispatcher	S					✓		✓			✓			
1.6	Remote cargo locking and unlocking by the dispatcher	S					✓		✓			✓			
2.1	Hazmat driver identification and verification by dispatcher	S	✓	✓											
2.2	Hazmat driver identification and verification by roadside safety enforcement officers	S	✓	✓											✓
2.3	Hazmat cargo location tracking by the dispatcher	S											✓		
2.4	Hazmat cargo route adherence by the dispatcher and roadside safety enforcement officers, as required, based on the quantity and type of hazmat being transported	S					✓			✓					✓
2.5	Untethered trailer notification and tracking by dispatcher	S									✓		✓		
2.6	Hazmat cargo tampering alert to the driver and the dispatcher	S							✓						
2.7	Remote cargo locking and unlocking by the dispatcher	S					✓		✓			✓			
2.8	Real-time emergency alert message notification by the driver to the dispatcher	S,T			✓	✓									
2.9	Real-time emergency alert message notification by the vehicle after the vehicle is involved in a crash														
2.10	Real-time emergency alert message notification by the vehicle to the dispatcher if vehicle senses an unauthorized driver	S	✓	✓											
2.11	Real-time emergency alert message notification by the dispatcher to local and state law enforcement officials and emergency responders	S,D, T	✓	✓	✓	✓				✓					✓
2.12	Remote hazmat vehicle disabling by the driver	S,T				✓								✓	
2.13	Remote hazmat vehicle disabling by the dispatcher	S					✓							✓	
2.14	Hazmat driver identification and verification by the vehicle if the vehicle is motionless for 10 minutes	S	✓	✓			✓								
3.1	Remote cargo locking and unlocking by the dispatcher	S					✓		✓			✓			
3.2	Hazmat driver identification and verification by the receiver							✓							
3.3	Hazmat cargo verification by the receiver	S						✓							
3.4	Receiver confirmation of received cargo to the driver and dispatcher	S						✓							
3.5	Auditable log of all shipments to be kept by the motor carrier														

Combining the selected hazmat materials and operational scenarios described above, with the technologies shown in Table 8 to address all the required functional requirements, a high-level system design was developed to meet the requirements developed as part of the Task 3 Requirements Analysis task. Figure 7 depicts the high-level system architecture for the Hazmat FOT. Detailed system- and technology-specific architecture diagrams can be found in the Hazmat FOT Task 4: System Requirements and Design Document (July 17, 2003).

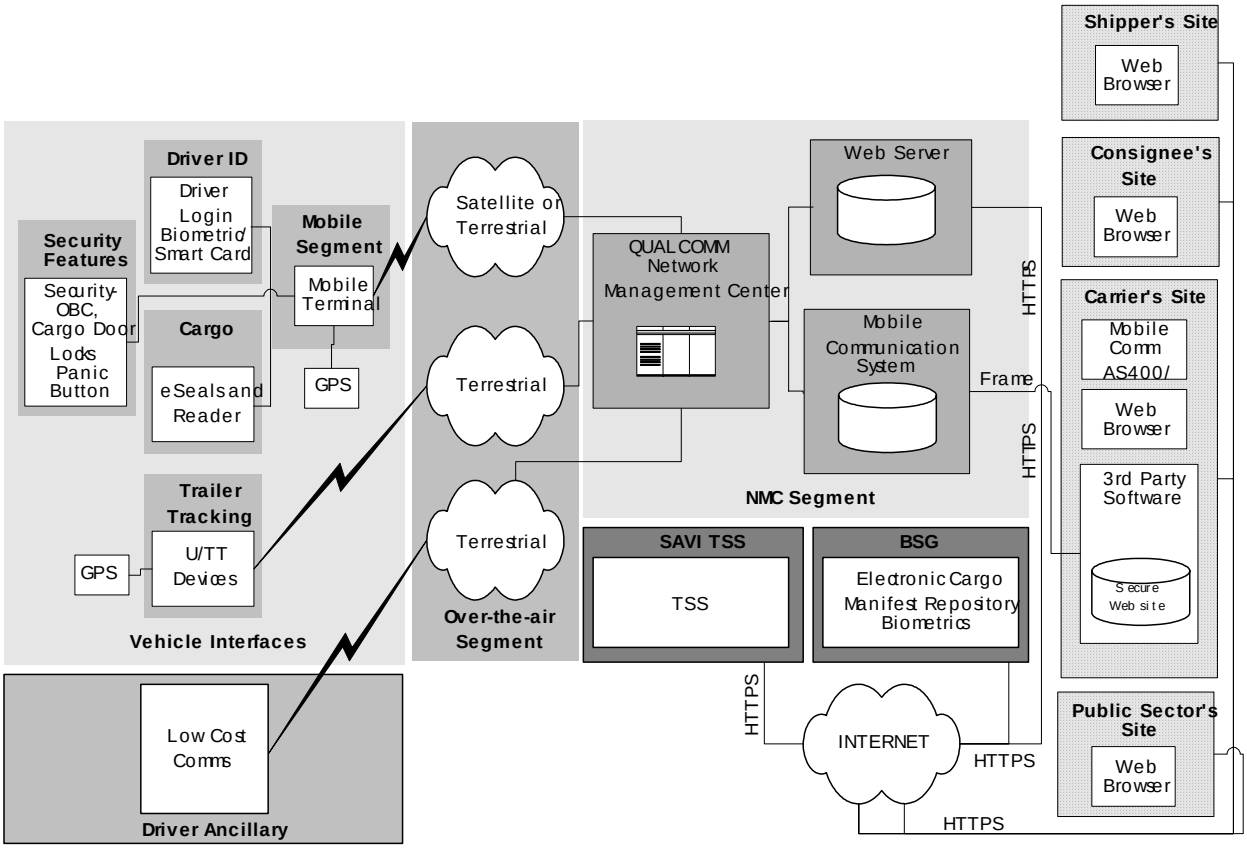

Figure 7. Hazmat FOT High-Level System Architecture Overview

4.0 Methodology and Conduct of the Field Operational Test

4.1 Overview

The discussion in Sections 3.2 and 3.3 outlines the approach used to put together the three building blocks of the FOT: the defined research objectives, the identified threats and vulnerabilities, and the applicable technologies. This section provides additional detail on that process and shows how the proposed scenarios were further defined and implemented.

4.2 Threat and Vulnerability Analysis

The identification of the threats and vulnerabilities of motor carrier hazmat transportation was presented in Section 2.4. This section describes the approach used to analyze that information, including the development of estimates for the potential damages that would result from terrorist use of hazmat in an attack.

4.2.1 Consequence Analysis

A typical security-based vulnerability analysis involves development of exposure values based on specific weapons and tactics. The analysis conducted for the FOT assumed worst-case outcomes for materials, defined reference components with specific vulnerabilities that can be exploited, and constructed attack profiles that can be used as the basis for defining test scenarios.

Further adaptation was necessary to address targets, which are ordinarily the focus of the analysis (such as critical facilities, sporting events, or monuments). To address the general use of hazmat as a weapon, it was necessary to conceptualize an ideal target for each material for each defined attack profile, much as a terrorist would. These idealized targets are not described in this report, as the information would provide a detailed blueprint for target identification, evaluation, and exploitation.

For the intentional release-based attack profiles, two sets of worst-case, material-specific consequence estimates were developed, one for bulk/truckload and one for LTL, primarily based on the different material quantities associated with each of these two operational types. These estimates are shown in Tables E-3 and E-4 in Appendix E. It is assumed that the release of the material being transported will result in worst-case consequences, which are not dependent on which specific tactic is used. The only exception to this is for interception, in which the terrorist cannot precisely place the hazmat prior to release, detonation, or ignition; therefore, consequences for these attacks would typically be lower than for theft or legal exploitation. Consequences estimates include deaths, injuries, and property damage and were developed from accident scenarios and expert judgment. They are designed to be order-of-magnitude estimates and to be relative rather than absolute.

For the unintentional releases, the results of the FMCSA risk study [3] were applied to an abbreviated list of the threat-based material classifications to allow comparisons. These consequences were expressed on an expected annual basis rather than on a single-incident, worst-case basis to reflect the nature of the risk assessment used to determine them. The consequences for unintentional releases also include other costs such as delay and evacuation costs. Table E-5 in Appendix E lists these costs for unintentional releases.

The consequence values for both intentional and unintentional releases include a cost-equivalent for fatalities and injuries of $3,000,000 and $215,000, respectively. These values were selected based on previous U.S. DOT hazmat impact studies. Rankings are sensitive to the total economic impact value of which these are a component in the calculations. These costs represent those that are recognized by the U.S. DOT for the purpose of analytical studies such as this one. A series of tables is presented in the full Task 1 report [2] with estimated consequences resulting from each combination of attack profiles (e.g., theft involving bulk/truckload operations) and each of the 18 threat-based material categories.

4.2.2 Results

The final step in the assessment process is to use the consequence estimates to develop a ranking of threat and material categories. In order to rank the various threat-based attack profiles against each other, two different sets of weights were applied to the consequence estimates. These weights were designed to reflect the attractiveness to a terrorist of (a) a specific attack profile relative to others and (b) a specific material for a specific attack profile. The two sets of weights are shown in Tables E-6 and E-7 in Appendix E. These weights take into account two sets of criteria: (1) the FBI criteria, which are focused on the attractiveness of a target and include the potential for mass casualties, significant economic damage, extensive psychological trauma, and high symbolic value, and (2) TSSI-developed criteria, which are focused on the attractiveness of the set of operations that a terrorist would need to employ to mount a successful attack. The ranking, shown in Table E-8 in Appendix E, provides an understanding of how the different attack profiles relate to each other and makes it possible to prioritize efforts to address the specific vulnerabilities that would allow terrorists to effectively carry them out.

In addition to ranking the attack profiles themselves, it is possible to rank the threat-based material categories across all attack profiles based on their estimated consequences and weightings. The overall threat-based material category ranking, shown in Table E-9 in Appendix E, could be used to apply specific countermeasures to the top-ranked categories.

These rankings (and the specific vulnerabilities that were identified for each reference component) were provided as input to Task 2, the Concept of Operations. They were an important consideration in defining operational scenarios and associated countermeasures that were selected for testing during the field operational test.

To use past history as a barometer or forecaster of future events, it is necessary to have a sufficiently large number of historical events upon which to base such a prediction. Without a sufficiently large historical record of terrorist events exploiting hazmat, it is difficult to predict with certainty the likelihood of any specific type of incident. It is instructive, however, to

compare the expected annual consequences of unintentional releases to the relatively large theoretical consequences of just one terrorist incident.

The FOT, and the companion cost-benefit analysis, address security, safety, and efficiency within the same context. It is likely that some protective measures applied to security vulnerabilities will provide benefits in safety and efficiency and these additional benefits will facilitate the adoption of these protective measures by industry.

The threat and vulnerability assessment framed the safety and security risks being addressed by the FOT and was the basis for developing the Concept of Operations (Task 2). In addition, the assessment categorized the threats and serves as a benchmark for the prioritization of potential countermeasures.

4.3 Scenario Development

As discussed in Section 3.2, the threat and accident-related profiles were compared with the four proposed scenarios to ensure that each of the profiles corresponded to at least one scenario. This was found to be the case and no adjustments to the scenarios were necessary. Including four scenarios in the FOT allowed the application of technology to a wider range of practical situations. The technology applied to each scenario to address the identified vulnerabilities could be tailored to the unique operational characteristics of each.

4.4 Deployment – Technologies and Operational Considerations

The Battelle Team included private sector technology providers that could offer products and/or services that would test one or more of the specified research objectives. Table 10 highlights the array of COTS technology brought to this test by these private sector partners.

Table 10. COTS Technology Providers

Team Member	Functional Capability	Brief Description
Qualcomm	Wireless communication (satellite, terrestrial, and digital), vehicle tracking and messaging	Qualcomm provided the infrastructure, hardware, and software to support wireless communication between the truck and the Network Management Center, the software interfaces that allow third parties to write interfaces to Qualcomm's mobile terminals and the onboard cargo, which allow control of the vehicle subsystems, including the trailer door locks and the vehicle immobilizer.
Saflink	Driver identification, verification, and cargo tracking system	Biometric smart card technology providing two-factor identification capability and the integration of an electronic supply chain manifest application.
Savi	Cargo identification and verification during shipment and electronic seal integrity	RFID devices capable of integrating with onboard wireless communication to monitor seal integrity of the cargo container.

Team Member	Functional Capability	Brief Description
Spill Center	Electronic Emergency Response Management Systems – Public Sector Reporting Center (PSRC)	Spill Center provided the PSRC technology and infrastructure which enable motor carriers and public sector agencies to create customized alert notification rules and receive alerts based on event data generated by on-board telematic devices. Spill Center's call center, web services, and software interface with wireless communication technologies and deliver near-real time alerts and include driver, vehicle, location, route, bill of lading and panic information. Carriers and public sector agencies use the PSRC technology to leverage and deploy existing safety and response resources.

4.4.1 FOT Design Criteria

The discussion below presents a high-level summary of the design criteria and requirements addressed in the development of the FOT. A more detailed, in-depth discussion of the overall FOT design can be found in the two Task 4 System Requirements and Design (SRD) documents [4,5].

The design criteria and rationale for how the Battelle Team approached addressing the requirements spelled out in the statement of work was to insure first that all applicable research objectives were addressed. The focus then turned to applying this technology to as broad a spectrum of hazardous materials as possible within the constraints of the program resources.

In selecting the technologies to test, it was important that the technologies be as close to COTS as possible. While it was not an absolute requirement that all technologies be commercially available at the time of the FOT, it was important that the technologies be more than just a concept or early beta-test candidate.

4.4.2 Technology Components

The discussion below presents a high-level description of the functionality of each technology component included in the FOT. A more detailed description of the technologies can be found in the two Task 2 Concept of Operations reports [6, 7] and the SRD.

Communication

Qualcomm provided the major technologies used as the backbone communication systems. These included satellite and terrestrial communications with global positioning system (GPS) and tracking capabilities, and digital mobile phone technologies without GPS. These are clearly "off-the-shelf" systems that are used by thousands of fleets throughout the world. In North America, more than 250,000 trucks use Qualcomm systems. Other major communication (integrated) systems would likely add another 100,000 vehicles to this grouping. When cell phones and two-way radios are included, nearly 100 percent of all 5-axle tractor trailer vehicles utilize wireless communications.

Wireless Satellite or Terrestrial Communications (w/GPS) and Tracking

Trucks received wireless tracking and communications systems with an integrated Global Positioning System (GPS) working in conjunction with the dispatch systems that provided for load/cargo positions and status. The system (Figure 8) also included a Driver Interface Unit for two-way text communications. Positions were automatically displayed for the carrier's dispatcher at a regular frequency determined by the carrier.

Figure 8. Wireless Satellite

These positions were viewed through an application that enabled the carrier's dispatcher to view the location of the vehicle on a map. Position information including the latitude, longitude, and time were also provided. The application enabled the carrier's dispatcher to track the vehicle in near real-time and also view a history of the vehicle's location at a particular time during the route.

FMCSA's 1996 ITS/CVO Cost-Benefit Study showed that wireless vehicle tracking was one of the fastest growing technologies in the trucking industry. It was also listed as having one of the highest return on investment for carriers that invested in asset tracking and communications systems.

Digital Phone (without GPS)

This technology provided integrated work order assignment and status messaging between a carrier's dispatcher and a driver using a low-cost digital cellular handset (Figure 9) with specialized operating software. Store-and-forward guaranteed messaging ensured message delivery upon returning to digital cellular coverage areas.

Figure 9. Digital Phone

Along with messaging, ancillary services such as mapping and directions were also available.

According to one American Trucking Associations' study, cell phones are now the most frequently used communication system in trucking. One issue that must be considered is the safety impact of using cell phones. At least one HMFOT test carrier forbids the use of cell phones in trucks because of safety (accidents) concerns. Many other carriers are investigating the safety issues associated with using a cell phone while driving, and a number of municipalities have banned the use of cell phones while vehicles are in motion.

Panic Buttons

Panic buttons existed in some communication systems prior to 9/11, but in general their integration and use has been limited. However, many new communications systems now include them as standard features, there is little collective knowledge on how often they are used.

Panic buttons provided real-time emergency alert message notification by the driver to the dispatcher. An emergency alert message was generated via the use of a panic button, which came in two configurations:

- A panic button mounted inside the vehicle to send an emergency alert (Figure 10).
- A wireless panic button (WPB) that can be carried by the driver to remotely send an emergency alert and/or use the remote panic button to disable the vehicle (Figure 11).

Figure 10. Dash Mounted Panic Button

The functionality implemented with the panic buttons (either dash mounted or wireless) was configurable. Functions that could be enabled by pressing the panic button included:

- Disabling/shutting-down the vehicle
- Sending an emergency alert notification to the communications control center to be forwarded on to the carrier's dispatcher
- Bleed the air from the trailer's air-brake system
- Flash the vehicles lights, honk the horn, etc.

Figure 11. Wireless Panic Button

Driver Authentication

Driver ID systems, particularly on-board systems are extremely new to the trucking industry with very few operational systems in place. Nevertheless, driver authentication was included in the FOT to ensure that only authorized drivers were operating hazmat vehicles and picking up hazardous materials shipments. This FOT tested two separate technologies designed to authenticate drivers.

Driver Authentication with Global Login

Similar to a username and password on a computer system, Global Login is an authentication feature of the Wireless Communications System. Through the use of a driver login process, the login information (user id and password) that the driver enters into the truck-based interface was verified both locally (on the truck) and over the air using the wireless communication system. If this verification fails, various configurable alerts and resulting actions were triggered up to and including vehicle disabling with the aide of an on-board computer (if installed).

Driver Authentication with Biometric Verification

This technology required having a biometric verification unit (Figure 12) on the vehicle. This was a customized system designed to satisfy the environmental and usage characteristics required for installation in a trucking rig. The biometric system consisted of a Central Processing Unit (CPU) with proprietary firmware which controls an attached smart card reader and fingerprint scanner, and which performs biometric verification. The biometric system was customized to communicate with the on-board tracking and communications system.

Figure 12. Biometric Identification

Electronic Supply Chain Manifest (ESCM)

Supply chain management software is a major component of the business industry, although it continues to grow and evolve in sophistication. However, supply chain systems have only recently integrated with onboard systems, and even fewer supply chain systems link with the public sector. When personnel ID and smart cards are included, the research team was not aware of any off-the-shelf systems for managing these different requirements. The US DOT-sponsored ESCM system does provide technologies that allowed positive identification of the person responsible for the cargo and tracking capabilities for cargo movement within a hazardous materials shipment. Combining biometric verification, smart-cards, Internet applications and the on-board wireless communications, the system insured proper chain-of-control for the hazardous materials throughout the lifecycle of a shipment. It also provided visibility into the location and status of the shipment to the shipper, carrier and consignee, thus enhancing both security and customer service.

Electronic Supply Chain Manifest (ESCM) system security was achieved using:

- Biometric fingerprint readers to restrict unauthorized system access and validate driver identification. Biometric log-ins were required at all access points to create, modify, send, receive, or view data and information within the enclosed test system; and

- Smart cards that integrate data encryption and biometrics to enhance security of the ESCM system. Encrypted smart cards containing shipper, cargo, and driver data were used throughout the ESCM supply chain to transfer and validate essential supply chain information.

Remote Vehicle Shut Down

The ability to remotely control or shut down a vehicle has existed for many years but has seen very little use in the United States, partially due to cost and few historical precedents for justifying the investment. The FOT included an intelligent onboard computer (OBC) integrated with the wireless communications and vehicle operating systems to allow a variety of security related functions, based on configurable input. The OBC was used to control the disabling of the vehicle in a variety of means. These methods included blocking fuel, or sending proprietary system instructions via the wireless communications system directly to the vehicle's data bus. The primary mode of disabling for this FOT was retarding the vehicle into a limp mode where the vehicle still has electrical power but little throttle response past idle. The actual mode of disabling depended on the make, model, and year of the vehicle during installation. The OBC was also configured to shut the vehicle down if there was a loss of satellite signal strength (i.e., severed feed cables). The driver also was able to call the monitoring center and inform them that the vehicle needs to be disabled (in case of theft, for example). At that time the dispatcher could send an over-the-air command to disable the vehicle.

Cargo Door Locking

A cargo door lock (Figure 13) that required the driver to request authorization from the carrier's dispatcher to lock or unlock the trailer door was also demonstrated. This lock was a rugged unit that was bolted to the inside door of the trailer. Using over-the-air communications, a message requesting the doors to be unlocked/locked was sent to the dispatcher. The dispatcher then sent a message to the vehicle OBC device, which sent a command to the door, allowing the driver to unlock/lock the cargo door. For more than 20 years, sophisticated cargo door locking systems have been on the market, however standard, low-cost seals, bolts and locks continue to dominate the market.

Figure 13. Cargo Locking

Electronic Cargo Seals

"E-seals" are a ubiquitous category of sophisticated seals that identify tampering, and/or create random access codes. The type of seal used in the FOT is very sophisticated in its design, but

cost and technology integration issues have nearly precluded its use in the for-hire trucking industry.

This technology included a cargo E-seal (Figure 14) that automatically generated an alert if the seal was broken without proper authorization. The seal used short-range wireless communications to interface with a mobile E-Seal reader (located in the vehicle). The mobile reader was connected to the on-board wireless communications device and the cargo alerts were forwarded automatically to the dispatcher. These alerts included the date, time, and location where the seal was breached.

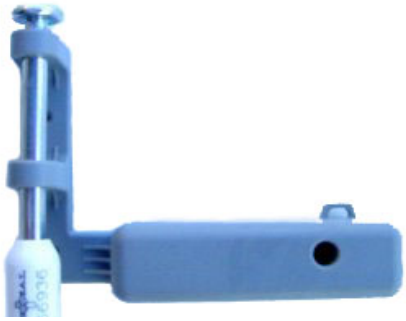

Figure 14. Smart Seal Tag

The driver was alerted of the security breach by one of three ways:

1. Dispatcher sent a message to alert the driver
2. The hand-held device had a driver display
3. The system was integrated with the OBC and was hooked to a buzzer to alert the driver

Geofencing

There are a variety of ways to create geofencing around vehicles and facilities, and there has been some specialized use of this concept in the past; mostly for high-security facilities. While there is now great interest by the public sector in utilizing geofencing for HM vehicles, the technology – particularly the system algorithms – are still developing. Consequently there are few robust systems available today.

Within the FOT, this technology deployed specialized software that allowed the operator to define a risk area or a route to monitor. An "electronic fence" was set around any given route or point on a displayable map (Figure 15).

The dispatcher could define a risk area (e.g., the White House) and if the vehicle entered the risk area or deviated from its route, an alert was sent to the carrier's dispatch center. A safe-haven could also be setup as a geofenced area and notifications could be configured if a vehicle left the area.

The geofencing capability interacted with frequent positioning and the on-board wireless communications system. If the geofence application had received a security breach, the system would automatically increase the positioning reports to a configurable time interval.

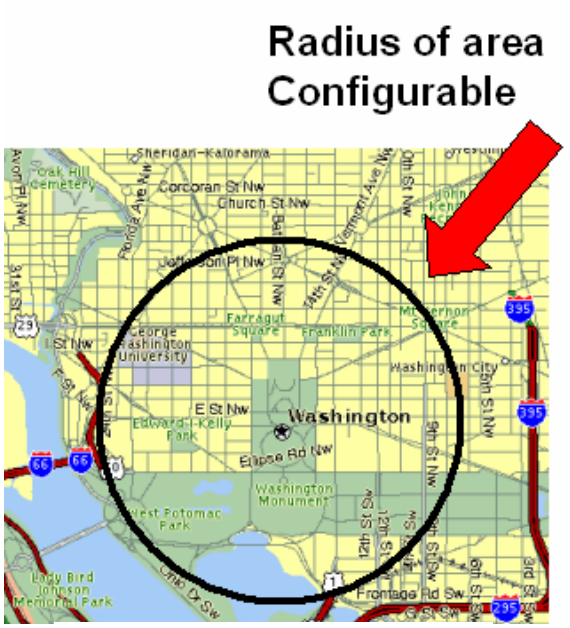

Figure 15. Geofencing

Trailer Tracking

Figure 16. Trailer Tracking Subsystem

Trailer tracking systems have existed for approximately 10 years but only recently – with the advent of integrated asset management software – has the industry begun investing in trailer tracking on a fleet-level scale. The FOT trailer tracking subsystem (Figure 16) provided trailer position information to the dispatcher on a regular basis.

The collection of untethered trailer positioning information was accomplished through the installation of devices on the trailers. Through the use of various sensors, these devices monitored the trailer to which they were attached. In response to physical or temporal events, these devices reported details of the event, including position, time, status, and identity data.

Figure 17. Tethered Device

Using the tethered device (Figure 17), connect and disconnect events were captured and transmitted as alerts to the dispatcher. This notified the dispatcher that a trailer had been connected or disconnected from the tractor.

Public Sector Reporting Center (PSRC)

The Battelle Team created the PSRC in order to provide advanced capabilities to law enforcement for data acquisition, fusion, and distribution of messaging for enhancing hazardous materials safety and security. During the FOT, the center was staffed live, 24/7, and was able to incorporate wireless voice/data communications, satellite-tracking technology, automatic routing of alerts to authorities, and online access to highly specialized data. The results were real-time alerts based on monitoring of hazmat shipment information, increased load security, and enhanced law enforcement actions and incident response in the selected test areas.

The PSRC made available the web-based application and allowed end users to create and manage rules that specified which conditions triggered the alert and sent the notification messages. The PSRC also managed user contact information including email, voice text messaging on cell phones (vtext), fax, and pager numbers.

The dominant technology for the PSRC included intelligent agent software as well as database and messaging software which produced and delivered alerts based on detecting certain user-specified events.

The system accepted information input in the form of data feeds from a number of different sources, namely FOT partners. The information from each partner source was temporarily stored and preprocessed. The data was then aggregated and stored in the newly created data silo (a single relational database). The data silo correlated and stored all the information received from the various data feeds. Once in the data silo, a software program acting like an intelligent agent, analyzed the individual pieces of information according to customized rules. These rules analyzed the contents of the data silo, finding data patterns or specific criteria defined by users.

As those patterns were found and criteria were met, the system sent one or more messages according to a user specified distribution list.

The PSRC provided the following functionality to motor carriers and public sector agencies:

- Participating motor carriers and agencies created custom alert notification rules based on off-route, unauthorized driver and panic event data. Event data was generated by on-board telematic devices and delivered to the appropriate carrier and public sector agency in the form of a customized alert.

- Numerous individuals within each motor carrier and agency created custom alert notification rules such that each individual or department would receive each particular alert by their choice of email, fax, page, text message, and voice.

- Using hand-held devices and cell phones, the participating carriers and agencies were able to update the PSRC with contact information; view carrier, load, driver and location information; and receive email, text message, and voice alerts.

- Carriers were able to create customized alerts and designate alert levels consistent with specific company operations and protocols. The ability for an unlimited number of individuals within the company to receive customized alerts based upon a particular business activity, load, or customer enabled the carrier to leverage existing carrier safety and response resources efficiently.

- Public sector enforcement and response agencies were able to create customized alerts and designate alert levels consistent with agency enforcement and response protocols and procedures. The ability for an unlimited number of individuals and departments within the agency to receive customized alerts based upon a particular event, material or location enabled the agency to maximize personnel and identify and respond to priority events more effectively.

4.4.3 Technology Selection Rationale

The deployment team recognized early on in the FOT planning stages that the unique operational characteristics of many of the hazardous materials carriers around the country would not lend themselves to full-scale deployment of all the technologies included in the test. While it may be prudent (and the market may bear the cost) to deploy more technologies on certain types of shipments (e.g., explosives), other carriers operate on thin profit margins and the marginal cost of deploying some of these technologies in their vehicles would be prohibitive. To represent these concerns of the market, the FOT separated the various technology components into six technology tiers, ranging from a low-end cost of approximately $250 per vehicle to a high-end of approximately $3,500 per vehicle. Table 11 provides a brief summary of each technology tier.

Table 11. Technology Tiers

Focus	Management System
1 (Low-end, approximately $250 per vehicle)	Include a digital cellular phone with pickup and delivery software with phone/on-board directions/mapping. This option would also include on-site vehicle disabling with the wireless panic remote. This would not be able to send a panic message but would give the ability to shut it down remotely. This would not include positioning until position location is implemented by the national networks.
2 $800	Includes terrestrial communications with in-dash panic button.
3 $2,000	Includes satellite communications with an in-dash panic button and global login.
4 $2,500	Includes all of what is in tier 3 but adds the OBC. A second variant included in this tier includes satellite communications with an in-dash and wireless panic button with biometric authorization, and E-manifest.
5 $3,000	Includes satellite communications with an in-dash and wireless panic button with biometric authorization, E-manifest and an additional OBC. The other variant is swapping the OBC for an untethered trailer tracking device.
6 (High-end, approximately $3,500 per vehicle)	Includes satellite communications with an in-dash and wireless panic button with biometric authorization, ESCM, and E-Seals.

These estimates for the each end of the price continuum represented only the hardware installed on the trucks in commercial quantities. They did not reflect the price of servers and dispatch systems amortized over the number of vehicles since this can vary widely depending on customer setup.

4.4.4 Scenario Development

The FMCSA required addressing specific research objectives with technologies deployed onto 100 commercial trucks. In addition, from an operational perspective, it was important that the technology applications tested be representative of the various hazmat industry segments and the unique operational considerations of each. Based on the risk profiles and route components identified during the risk and threat assessment, four operational scenarios were developed for the FOT. Table 12 presents a summary of the scenarios and technology components deployed per scenario. Each scenario consisted of 25 vehicles.

Table 12. Technology Components by Scenario

Scenario	Description	Technology Components	
1	Bulk Fuel Delivery	• Wireless Satellite Communication • Global Login • In-Dash Panic Button • Wireless Panic Button	• Digital Phone • Terrestrial Communication • On-Board Computer • PSRC
2	LTL High Hazard	• Wireless Satellite Communication • Global Login • In-Dash Panic Button	• Wireless Panic Button • Terrestrial Communications
3	Bulk Other	• Wireless Satellite Communications • Biometric Verification • In-Dash Panic Button	• Wireless Panic Button • Electronic Supply Chain Manifest • PSRC
4	Truckload Explosives	• Wireless Satellite Communication • Biometric Verification • In-Dash Panic Button • Wireless Panic Button • Electronic Supply Chain Manifest	• On-Board Computer • Wireless Electronic Cargo Seal • Geofencing • Untethered Trailer Tracking • PSRC

To further leverage the available technologies and involve a wider range of participants, these scenarios were subdivided into different components. Table 13 identifies the participants in each scenario and the number of vehicles that were involved.

Table 13. Scenario Participants

Scenario	Vehicles	Shipper	Carrier	Consignee	Public Sector Agencies
1a	13	ExxonMobil	Dupre Transport	Various	Texas Department of Public Safety
1b	12	ExxonMobil	Cox Petroleum	Various	California Highway Patrol
2a	12	GE Betz	Distribution Technologies (DisTech)	Various	None
2b	13	GE Betz	Roadway Express	Various	None
3a	12	DOW Chemical	Transport Service	NuFarm Americas	None
3b	7	BP Chemical	Quality Distribution	None	None
3c	6	BP Chemical	Roeder Cartage	Evans Chemical	New York State Police
4a	12	Orica USA	R&R Trucking	Orica Nitrogen	Illinois State Police
4b	13	Dyno Nobel	Dyno Transportation	Alpha Explosives	

4.4.5 Design and Installations

The implementation plan addressed the following topics:

- Overview of the FOT
- Training requirements for both deployment team and participant personnel
- Implementation details for each scenarios, including a management plan, roles and responsibilities, an installation plan, and a training plan
- Support processes for both the deployment team and for the participants, including a hotline and engineering support
- Procedures for technology upgrades and addressing equipment failures during deployment
- Internal management and accounting issues.

Processes and Dates

Training of FOT management personnel for scenario 1 and 2 were held in San Diego on August 5th, 2003. A second group for Scenario 3 and 4 was trained on August 21st and 22nd, 2003. These were staged further apart so the training data were still fresh prior to launching the particular scenarios. The training included the implementation plan as well as carrier, shipper, and driver training guides.

Figure 18 shows the installation dates of each carrier's hardware along with the removal dates.

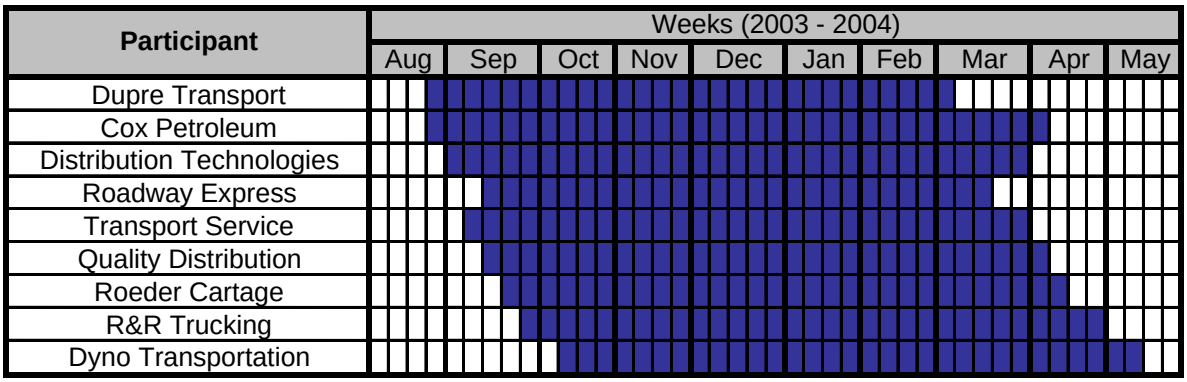

Figure 18. FOT Technology Installation, Operation, and Removal Schedule

Support and Training

Each carrier was assigned a Qualcomm regional Customer Service Representative (CSR) to manage, support, and train the participants. The CSR was on site for installs, training, and ongoing visits throughout the six-month test. A Saflink CSR was also on-site for Scenarios 3 and 4 installations of the ESCM system and related technologies.

The training provided by the CSRs included instructing the participants on the roles for carriers, drivers, state agencies, and the deployment team. It also included the collection of test data from the participants to support both the deployment (by uncovering any implementation issues) and the independent evaluation (cost/benefit analysis).

Table 14 shows the record of training dates and launch dates of each scenario:

Table 14. FOT Training Schedule

Scenario	Participant	Training Dates	Launch Dates
Scenario 1a	Dupre	Week of August 25th	9/2/2003
Scenario 1b	Cox	Week of August 25th	9/2/2003
Scenario 2a	DisTech	Week of September 8th	9/12/2003
Scenario 2b	Roadway	Week of September 15th	9/15/2003
Scenario 3a	Transport Services	Week of September 15th	9/24/2003
Scenario 3b	Quality Carriers	Week of September 22nd	9/25/2003
Scenario 3c	Roeder Cartage	Week of September 29th	10/2/2003
Scenario 4a	R&R	Week of October 6th	10/14/2003
Scenario 4b	Dyno	Week of October 12th	10/27/2003

Each CSR was also responsible for setting up all on site evaluations with the evaluators as well as ongoing training when and if needed per carrier.

4.4.6 Conduct the FOT Beta Test

The Battelle Team conducted a beta test of the FOT on July 14-18, 2003 at Qualcomm headquarters in San Diego, CA. The beta test utilized the Qualcomm technology truck and included members of the Deployment Team and the Independent Evaluation Team, led by Science Applications International Corporation (SAIC). A full description of the beta test is presented in Appendix D.

The FOT system design documents [4,5] were modified as a result of the beta test and full-scale deployment of the FOT occurred between August 2003 and May 2004. Throughout the field test, there was close integration with the independent evaluators. A complete description of the four scenarios that comprised the FOT is presented in Appendix A. This includes the participants, the specific technologies that were installed on each truck, and a general description of how the technologies were used in the day-to-day operational setting of the participants.

4.4.7 FOT Data Collection

Throughout the field operational test, a variety of data was collected from the deployed technologies. Well over one million data points were collected. The type and format of data was refined several times based on initial data analysis conducted during the 2003 beta test. A data distribution plan forwarded all data to the Battelle research team, FMCSA, and to SAIC, the project's Independent Evaluation Team. Prior to distribution, a joint ATRI/SAIC data group continually analyzed data and questions and/or issues, and worked with the data system integrators and vendors to clarify or revise data presentations, or investigate system usage. For example, if a specific technology was not producing adequate data, the Deployment Team would investigate and determine whether follow-up training was necessary or if there was an issue with the technology itself. This ensured that data points would support the analysis component of the project. Data was collected on a monthly basis.

Not all technologies produced "operational" data streams. Several technologies were tested both in staged testings in-person and during company visits. Due to lack of integration, data was mined from three separate databases: Qualcomm, Savi, and BSG. The following technologies provided data streams:

- Electronic Supply Chain Manifest – System tracked document creations, electronic cargo data transfers, data confirmation and verification, verified and authenticated system users, and documented changes in cargo "chain of possession."

- Wireless Satellite and Terrestrial Communications (w/GPS) – Produced forward and return messages as well as vehicle positions.

- Wireless Terrestrial Communications Handheld w/ pickup and Delivery Software – Produced and managed information macros and vehicle positions.

- Driver Authentication with Global Login – System created information on driver login/logoff, bad login, distance exceeded, time exceeded, and driver bumped off events.

- Tethered Trailer Tracking – Trailer events (connect or disconnect), as well as position reports were collected.
- Untethered Trailer Tracking – Trailer position reports were collected.
- Electronic Cargo Seals – Sealed, unsealed, and tampered seals were all reported and in turn generated a position report.
- Routing and Geofenced Mapping Software – Out-of-route and exception based violations were reported with position reports.
- Dash and Wireless Panic Buttons – Panic messages were triggered and stored by depressing the panic buttons and collected.
- Cargo Door Lock – Position reports and lock and unlock messages were collected.

4.5 Addressing Functional Requirements

The remainder of this section provides a description of the FOT approach for addressing each of the functional requirements (FR). It identifies the technology products, the participants, and the scenarios that were applied to address each FR as well as the operational approach taken to test each technology either in a daily operational environment or a staged event test.

Table 15 identifies the shippers, carriers, consignees, and hazmat product for each scenario and sub-scenario of the FOT.

Table 15. FOT Participants by Scenario

Scenario	Shipper	Carrier	Consignee	Hazmat Product
1a	Exxon Mobil	Dupre Transport	Various	Class 3 (Flammable Liquids) delivered in and around a 100-mile radius of Houston, Dallas, San Antonio, and Austin, Texas.
1b	Exxon Mobil	Cox Petroleum	Various	Class 2 (Flammable Gas) and Class 3 (Flammable Liquids) delivered in southern and central California region ranging from San Diego north through the Bay Area to Sacramento.
2a	GE Betz	Distribution Technologies	Various	Hydrochloric Acid (Class 8) delivered from Macon, Georgia to various consignees in Tennessee, North Carolina, South Carolina, and Florida.
2b	Various	Roadway Express	Various	Various LTL high-hazard loads out of Roadway's operations in San Diego, CA.

Scenario	Shipper	Carrier	Consignee	Hazmat Product
3a	DOW Chemical	Transport Service	NuFarm Americas	Bulk chemical delivery of HM Class: 9 2, 4, D Ester on routes originating in Midland MI and delivered to consignees in Illinois, Missouri, Indiana, and Ohio.
3b	BP Chemical	Quality Distribution	None	Bulk chemical delivery of Class 3 Flammable and Class 2.2 Non-Flammable with inhalation hazard on routes originating in Lima, Ohio and delivered to consignees in Kentucky, Tennessee, Arkansas, and Texas.
3c	BP Chemical	Roeder Cartage	Evans Chemical	Bulk chemical delivery of Acrylonitrile (AN) Class 3 Flammable and poison with routes originating in Lima, Ohio and delivered to consignees in Illinois and New Jersey.
4a	Orica USA	R&R Trucking	Scenica USA	Class 1.1 – 1.6 Explosives with routes originating in Indiana and delivered to Morris Illinois.
4b	Dyno Nobel	Dyno Transportation	Dyno Nobel	Class 1.1 – 1.5 Explosives originating in Carthage, Missouri with deliveries to Lincoln, California.

4.5.1 FR 1.1 Hazmat Driver Identification and Verification by the Shipper

This FR required the application of technologies that could allow shippers to positively identify a driver prior to allowing that driver to take control of a hazardous materials shipment.

Two technologies, global login and biometric verification, were deployed to provide shippers the ability to verify the identity of a driver prior to allowing him/her to take control of a hazardous materials shipment.

Global Login – Used by itself, the global login required the shipper to watch the driver log in to the Qualcomm system in the cab of the vehicle using the mobile communications terminal. If the driver successfully logged in (proper username and password) a text message was received on the Mobile Communications Terminal indicating a successful login. If the driver entered an incorrect username and/or password, an error message was sent and the driver was required to re-enter the username and password.

The process[8] used to test this feature involved the following steps:

1. Driver initiates sequence by logging into Qualcomm system.
2. Driver is authenticated via use of proper username and password or is required to try again if login attempt failed.

[8] A more detailed description of the global login processes and test points (and all other technology test points) can be found in the Task 2 Concept of Operations (April 18, 2003).

3. When the system is initiated the driver receives an audible warning and message prompting him/her to login.
4. If the driver starts the engine but does not successfully log into the system after five minutes of idling, a global login security breach is sent to the carrier.
5. If the driver departs without successfully logging into the system after driving one mile, a global login security breach is sent to the carrier.
6. If the driver fails to successfully log into the system three consecutive times, a security breach is sent to the carrier.

The global login technology was used to address FR 1.1 in scenarios 1a, 1b, and 2a. Testing the global login feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during site test visits at Cox, Dupre, and DisTech in December of 2003. The second onsite tests were performed in February, 2004 for Dupre and March, 2004 with Cox and DisTech. All verifications of this functionality were performed at a carrier location with the independent evaluators serving the role of the shipper.

During the on-site tests the evaluators observed both successful and unsuccessful usage of the global login system. A successful use of global login was defined by when the user entered his/her username and password correctly and was granted access to the system. An unsuccessful login could be caused by entering either an incorrect username, a password, or entering an invalid username and password. When a login was unsuccessful (for whatever reason) the system prompted the user to re-enter his/her username and password. Three consecutive failed login attempts (number was configurable) were deemed to be an unauthorized attempt to access the system and an alert was generated. All events (successful and unsuccessful login) were captured successfully and electronic data was delivered to the independent evaluators as part of the monthly data deliveries.

Biometric Verification – The biometric verification system required the driver to pre-register in the system. This involved recording his/her fingerprint electronically into the biometric database as well as providing him/her with a wallet-sized smart card that contained an electronic copy of their fingerprint.

Driver verification at the shipper's location using biometrics was accomplished two different ways. Some shippers had desktop computer systems with biometric fingerprint readers (bioboxes – see Section 4.5.2 for details) attached. Others simply watched the driver perform the biometric verification in the cab of their vehicle. The process for verification was the same for both approaches:

1. Driver inserts smart card into the slot on the biobox and then places his/her finger on the scanner for verification.

2. An initial verification is made locally, matching the fingerprint stored on the smart card to that scanned on the biobox. If those two fingerprints match, the LED light begins flashing green. If they do not match, the LED light turns red.

3. Once the local verification is made, a message containing the driver's global login user name and password is sent to the Qualcomm Network Management Center (NMC) for verification. The NMC would then send a notification to the carrier, and when verified, a message would be sent back and the driver's identification would be displayed next to the vehicle name. The biobox LED would then turn to a solid green.

4. If the driver starts the engine and did not log in via biometric verification, after two minutes an audible beep is generated and after five minutes or one mile driven, a global login security breach is sent to the carrier.

The biometric verification technology was used to address FR 1.1 in scenarios 3a, 3b, 3c, 4a, and 4b. Testing the biometric verification feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during site test visits to Transport Services in December, 2003 and January, 2004. Site visits with Roeder were conducted in December, 2003 and January, 2004, with Quality in December, 2003, with R&R in January, February, and April of 2004, and with Dyno in January, 2004. All verifications of this functionality were performed at a carrier location with independent evaluators serving the role of the shipper.

During the on-site test, the evaluators observed both successful and unsuccessful usage of the biometric verification. On several of the occasions the driver's fingerprint was not always read on the first attempt and sometimes took several tries. All events were captured successfully and electronic data was delivered to the independent evaluators as part of the monthly data deliveries.

4.5.2 FR 1.2 Hazmat Cargo Verification by the Driver, Dispatcher, and Receiver

This FR required the application of technologies that would allow drivers, dispatchers, and consignees to verify the hazmat cargo. The primary technology application used to address this functional requirement was the Electronic Supply Chain Manifest (ESCM) system integrated with the biometric verification discussed above.

ESCM – The ESCM system provides a secure means for a shipper to generate a manifest, notify their selected carrier of the need for shipment, confirm that only authorized drivers gain access to a particular load, and only authorized shipments are delivered to the eventual consignee. The process for verification of the cargo is:

1. Shipper logs into the ESCM system with fingerprint and smart card to create electronic manifest.
2. System generates an e-mail to inform the carrier and consignee of the manifest ID (number within the ESCM system).
3. Carrier notifies the driver of load.
4. When driver arrives at shippers facilities, he/she logs into the ESCM with fingerprint and smart card to accept responsibility for the specific load/manifest.
5. System generates an e-mail notification to the carrier and consignee that the driver has "accepted" the load.

6. When driver reaches consignee's location, he/she logs into the ESCM system using smart card and fingerprint and transfers responsibility for the load/manifest to the consignee.
7. System generates an e-mail notification to the carrier, consignee, and shipper confirming receipt by consignee.

The ESCM technology was used to address FR 1.2 in scenarios 3a, 3b, 3c, 4a, and 4b, the shipper and a brief description of the Hazmat Product shipped. Testing the ESCM feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during state agency testing with BP, Roeder, Evans Chemical, Dyno, R&R, and Orica in February, 2004.

During the on-site tests the ESCM technology worked very well with some instances where driver's were required to re-insert their finger for successful biometric verification. The state agencies were able to pull up the electronic manifest from the roadside using a hand-held personal digital assistant (PDA) equipped with a wireless internet access card. In one test, the team also accompanied the driver inside of the consignee location to view the successful receipt process.

4.5.3 FR 1.3 Hazmat Driver Identification and Verification by the Vehicle

This FR required the application of technologies that required drivers to positively identify themselves in the vehicle prior to allowing that driver to take control of a hazardous materials commercial vehicle.

Two technologies, global login and biometric verification, were deployed to provide this vehicle-based identification and verification of a driver prior to allowing him/her to take control of a hazardous materials commercial vehicle.

Global Login – The global login process was identical to that described for addressing FR 1.1 above.

The global login technology was used to address FR 1.3 in scenarios 1a, 1b, and 2a. Testing the global login feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during site test visits (see discussion for FR 1.1).

Biometric Verification – Driver verification by the vehicle using biometric verification was identical to that described for addressing FR 1.1 above.

The biometric verification of the driver by the vehicle was tested in scenarios 3a, 3b, 3c, 4a, and 4b. Testing the biometric verification feature was accomplished during the daily operations of the shippers, carriers, and consignees. As discussed later in the findings, there were several operational issues related with the driver identification and verification that centered primarily around the use of the biometric verification technology. These problems included drivers feeling that the "box" took up too much space where it was installed, some problems with the "bio box"

reading fingerprints of certain drivers, and difficulty orienting the fingers properly so the bio box would "read" the fingerprint. The majority of these problems would be fixed if the system as a whole were designed to be operated in a rugged environment such as the trucking industry.

The test team collected data remotely on usage of this technology and verified the application and use during site test visits (see discussion for FR 1.1).

4.5.4 FR 1.4 Hazmat Driver Identification and Verification by the Dispatcher

This FR required the application of technologies that required dispatchers to have the capability to positively identify drivers in the vehicle prior to allowing that driver to take control of a hazardous materials commercial vehicle.

Two technologies, global login and biometric verification, were deployed to provide this vehicle-based identification and verification of a driver prior to allowing him/her to take control of a hazardous materials commercial vehicle.

Global Login – The global login process was identical to that described for addressing FR 1.1 above.

The global login technology was used to address FR 1.4 in scenarios 1a, 1b, and 2a. Testing the global login feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during site test visits (see discussion for FR 1.1).

All functionality was successfully performed at a carrier location with independent evaluators serving the role of the dispatcher observing a driver.

Biometric Verification – Driver verification by the vehicle using biometric verification was identical to that described for addressing FR 1.1 above.

The biometric verification of the driver by the vehicle was tested in scenarios 3a, 3b, 3c, 4a, and 4b. Testing the biometric verification feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during site test visits (see discussion for FR 1.1).

All functionality was successfully performed at a carrier location with independent evaluators serving the role of the dispatcher viewing a driver.

4.5.5 FR 1.5 Hazmat Cargo Tampering Alert to the Driver and the Dispatcher

This FR required the application of technologies that provided the drivers and dispatchers notification if their hazmat cargo was tampered with.

Two separate cargo security technologies (electronic seals and cargo trailer locking) were integrated with an on-board computer (OBC) technology that interfaced with the Qualcomm on-

board communications unit to provide the driver and dispatcher an indication if the security barrier had been penetrated or tampered with during transit.

OBC with Cargo Door Lock – This technology utilized a ruggedized door lock bolted to the inside door of the trailer. Locking and unlocking of this door lock was controlled remotely by the dispatcher. If the door was opened or tampered with prior to proper authorization, an alert was sent to the OBC and forwarded through the Qualcomm NMC to the carrier.

The OBC and cargo door lock technology was used to address FR 1.5 in scenario 4a. Testing the OBC/cargo lock feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during site test visits at the Illinois weigh station scale just across the border from St. Louis, MO in February, 2004. R&R Trucking provided their driver and vehicle for the test.

Electronic Seals – The electronic seal technology used involved the use of active electronic cargo seals that communicated using dedicated short-range communication (DSRC) to a hand-held reader. The reader included a cradle assembly that was integrated with the on-board communications unit. The handheld unit used by the drivers recognized the serial numbers of the tags "within range" of the unit. These tags were typically on the trailer door locks.

Once locked, the mobile unit monitors the status of the electronic seals, and if any seal is tampered with, the system automatically sends an alert over the air to the dispatcher. In addition, if at any time the seals can no longer be recognized by the mobile reader (i.e., the cab is disconnected from the trailer and physically separated), the system automatically sends an alert over the air to the dispatcher. If the driver is required to open the cargo doors while en-route (i.e., at an inspection station or roadside by a roadside safety enforcement officer), using the handheld unit the driver electronically "authorizes" the opening of the seals and the system records this opening in a history log. Once completed, the driver repeats the locking procedure and this information is also recorded in the history log.

The process for verifying proper operation of the cargo tampering capabilities of the electronic seals involved:

1. While in surveillance mode, if handheld detects tampering of one or more seals, an alert is sent over the air to the carrier and an audible alarm sounds in the cab of the truck.
2. If seal becomes undetected an alert is sent over the air to the carrier and an audible alarm sounds in the cab of the truck.

The electronic seal technology was tested in scenario 4a. Testing the electronic seal feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during site test visits at R&R in April 2004.

During the on-site tests for the hardened door lock the evaluation team did not test tampering of the door lock since that would have required damaging to door of the trailer.

The evaluation team did observe periodic difficulties being able to read the tags on the doors of a 48 foot trailer with stainless steel doors while testing the Savi seals. The tags were easily read if located on the doors while the doors were open facing the tractor. As discussed in Section 4.6, the e-seal manufacturer indicated that a newer generation e-seal resolves this issue.

4.5.6 FR 1.6 Remote Cargo Locking and Unlocking by the Dispatcher

This FR required the application of technologies that provided the dispatchers the capability to remotely control access to the hazmat cargo.

OBC with Cargo Door Lock – This technology utilized a ruggedized door lock bolted to the inside door of the trailer. Locking and unlocking of this door lock was controlled remotely by the dispatcher. When the driver wanted to lock/unlock the trailer, he/she would send a message via the on-board communication unit to the dispatcher. The dispatcher would be able to confirm that the driver was at the appropriate location and send a message back to the OBC authorizing the locking/unlocking and the OBC would send the appropriate command to lock/unlock the cargo door. The process for verifying proper operation of the OBC and cargo door lock included:

1. Driver sends an over-the-air message requesting trailer door lock.
2. Message is forwarded from Qualcomm NMC to carrier's dispatcher.
3. Dispatcher responds with authorization to lock/unlock cargo door.
4. Driver presses trailer door switch in cab and walks to back of trailer and opens door.

Note: Initial configurations gave the driver 20 seconds from the time he/she pressed the trailer door switch in the cab to get to the back of the trailer and open the door. If more than 20 seconds elapsed, the door automatically defaulted back to the locked position. During the initial beta test (see Appendix D for more details), this was found to be too short a period of time and the time was increased to 60 seconds for the operational test.

The OBC and cargo door lock technology was used to address FR 1.6 in scenario 4a. Testing the OBC/cargo lock feature was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during site test visits at the Illinois weigh station scale just across the border from St. Louis, MO in February, 2004.

During the on-site tests for the ruggedized door lock the evaluation team demonstrated that the door could not be opened unless the command was sent to the driver. The driver also successfully demonstrated that the door could be opened after receiving authorization and pushing the dash mounted switch which unlocked the back door.

4.5.7 FR 2.1 Hazmat Driver Identification and Verification by Dispatcher

This FR required the application of technologies that provided the dispatcher the capability to remotely identify a driver prior to allowing that driver to take control of a hazardous materials shipment.

Two technologies, global login and biometric verification, were deployed to provide dispatchers the ability to verify the identity of a driver prior to allowing him/her to take control of a hazardous materials shipment.

Global Login – The global login process for this FR is identical to that described earlier for FR 1.1 with the exception that the dispatcher monitors the login/logout activity remotely.

The global login technology was used to address FR 2.1 in scenarios 1a, 1b, and 2a. Testing this feature was accomplished in parallel with the testing described earlier for FR 1.1.

Biometric Verification – The biometric verification system process for this FR is identical to that described earlier for FR 1.1 with the exception that the dispatcher monitored the login/logout attempts remotely.

The biometric verification technology was used to address FR 2.1 in scenarios 3a, 3b, 3c, 4a, and 4b. Testing this feature was accomplished in parallel with the testing described earlier for FR 1.1.

4.5.8 FR 2.2 Hazmat Driver Identification and Verification by Roadside Safety Enforcement Officers

This FR required the application of technologies that provided the roadside safety enforcement officers the capability to verify the identity of a driver at the roadside. The technologies deployed to provide this capability again were the global login and biometric verification technologies described previously.

For the driver identification requirement, while en-route, the vehicle was stopped at inspection facilities and/or at the roadside by a mobile officer. In both cases, these stops were prearranged with the carrier, driver, and the roadside safety enforcement organizations and the testing was conducted in a "staged" environment. The driver identification occurred by one of three methods:

1. The officer watched the driver authenticate himself/herself using the global login feature on the vehicle.

2. The officer watched the driver authenticate himself/herself using the smart card and biobox reader installed in the truck.

3. The officer would bring the driver into an inspection facility or into a patrol car and use the smart card and biometric verification system installed there for verification of the driver's identity.

The global login technology was used to address FR 2.2 in scenarios 1a and 1b. Testing this feature was accomplished in parallel with the testing described earlier for FR 1.1.

The biometric verification technology was used to address FR 2.2 in scenarios 3a, 3b, 3c, 4a, and 4b. Testing this feature was accomplished during staged testing events at Evans Chemical, Roeder Cartage, and NYSP in Waterloo New York in February, 2004. The second on-site test verified the application and use during site test visits with R&R Trucking and Illinois State Police outside of St. Louis, MO in February, 2004. The carrier, driver and roadside safety enforcement officers were all notified in advance of this staged test.

4.5.9 FR 2.3 Hazmat Cargo Location Tracking by the Dispatcher

This FR required the application of vehicle and tracking technologies that provided the dispatcher the capability to monitor the location of a hazmat load. The technologies deployed to provide this capability were the basic Qualcomm QTRACS system and the tethered trailer tracking technology.

QTRACS – Qualcomm's QTRACS system monitors the location of the commercial vehicle. The on-board systems monitor their location using either GPS or QASPER (Qualcomm proprietary satellite-based location determination system similar to GPS). Position information is collected locally on-board the vehicle and transmitted via wireless communication to the NMC hourly[9]. Position locations (current and position history) were automatically displayed to the carrier's dispatcher through an application that allowed the dispatcher to view the location (latitude, longitude, and time) of the vehicle on a map.

This tracking capability was demonstrated using both satellite communications as well as terrestrial communications.

This technology was the foundation of the overall system integration and was used to provide cargo tracking to the dispatcher in all scenarios. Testing this technology was accomplished during the daily operations of the shippers, carriers, and consignees. The test team collected data remotely on usage of this technology and verified the application and use during all site visits.

Tethered Trailer Tracking – The TrailerTRACS technology monitored the connect/disconnect events and transmitted a message to the dispatcher when these events occurred. When a driver picked up a hazmat load and a connect message was sent, the dispatcher could then track that load along is route. As long as a disconnect message was not received before the load reached the consignee, the dispatcher was assured that the cargo was "connected" to the tractor sending the location information.

[9] The reporting rate is a configurable parameter with default frequency of one hour (configurable down to 10 minutes). The on-board unit collects and stores intermediate position locations and forwards all location information hourly.

The process for verifying proper operation of the tethered trailer tracking technology included:

1. When the driver hooked the tractor to the trailer, the tethered trailer unit transmitted an ID over the power bus to the mobile unit in the cab of the truck.
2. At this time, the trailer ID is displayed on the display unit in the truck.
3. The mobile unit would then send an over-the-air message to the carrier notifying them of the connect event.
4. This connect message is displayed to the dispatcher.
5. When the driver unhooks the trailer at the consignee's yard, the mobile unit detects the lack of the trailer track ID and sends an over-the-air disconnect message to the carrier.

Combined with the trailer tracking capability described above, this provided the dispatcher the capability to track the load and be assured that no unauthorized disconnects occurred while en-route to the consignee.

The tethered trailer tracking technology was tested in scenario 4b. Testing this technology was accomplished during the daily operations of the shippers, carriers, and consignees as well as during staged event testing. The test team collected data remotely on usage of this technology. The global search on-site testing was not performed with California CHP. One reason for this was the irregular demand requirements associated with this shipment. The load was specialized explosives that were only manufactured when Orica placed an order. Unfortunately, no orders were placed by Orica during the operational period. Other factors impacting the seasonality of these shipments related to the route of the shipment. The route included traversing the Donner Pass in western California, which is frequently closed due to sever weather conditions during the winter months.

4.5.10 FR 2.4 Hazmat Cargo Route Adherence by the Dispatcher and Roadside Safety Enforcement Officers, as Required, Based on the Quantity and Type of Hazmat being Transported

This FR required the application of vehicle and tracking technologies that provided the dispatcher the capability to track a hazmat vehicle's actual route compared to a planned route (on a map) and provide alerts to roadside safety enforcement officers when a geofence route is violated.

Geofencing – The geofencing technology was specialized software that interfaced with the Qualcomm vehicle location reporting information and allowed the operator (dispatcher or roadside safety enforcement officer) to define a risk area or a route to monitor. An "electronic fence" was set around any given route or point on a displayable map. The geofence could be either an inclusion zone (vehicle must stay within a specific defined area) or an exclusion zone (vehicle must not enter a specific defined area). The geofence areas were defined by the dispatcher prior to assignment of the hazmat load.

PSRC – The alerting process for roadside safety officers involved both dispatchers notifying appropriate officials when a geofence alert was received as well as the Public Sector Reporting Center (PSRC) automated alerting function. Prior to initiating a hazmat route, the carrier submitted trip plan information to the PSRC. When roadside safety enforcement officers had a vehicle pulled over (either roadside or at permanent weigh stations) they could use the hand held wireless devices provided by the PSRC to query the system and verify specific route adherence. In addition, when a geofence violation alert was generated by the dispatcher (automatic within the software application running at the carrier's facility), that alert would be forwarded to the PSRC. Based on the location of the vehicle and the safety enforcement organizations involved, the PSRC would then forward an alert to appropriate enforcement personnel via telephone calls, faxes, emails, and/or text messages (depending on how the individual enforcement personnel had defined their preference for receiving such alerts).

The process for verifying proper operation of the geofencing technology included:

1. Carrier initiated a route-based geofence trip on a designated route.
2. Once the trip is initiated, the host system "requests" position location information every 15 minutes (configurable parameter).
3. Dispatcher monitors the vehicle for positions and is able to view on a route map.
4. When driver deviates from the designated route over half a mile (configurable parameter), the host system begins requesting positions every five minutes.
5. If an exclusion zone is penetrated, the host system begins requesting position every 3 minutes.

Both the carrier's dispatchers, as well as selected dispatch officers, were provided with the appropriate software applications to allow them to view and monitor selected hazmat routes.

The process for verifying proper operation of the PSRC geofencing technology involved:

1. Roadside safety enforcement officer pulls driver over (either roadside or at permanent weigh station).
2. Using wireless handheld device, officer inputs vehicle specific parameters and can query the PSRC database for vehicle's adherence to required route.

The process to test the proper operation of the PSRC geofence alerting function included:

1. Alert is generated by dispatcher and forwarded to PSRC.
2. PSRC system correlates the vehicle, cargo, driver, and location with appropriate roadside safety enforcement officers.
3. Alert is generated and forwarded to appropriate roadside safety enforcement officers via telephone calls, faxes, emails, and/or text messages (depending on how the individual enforcement personnel had defined their preference for receiving such alerts).

The geofencing technology and alerting capabilities were tested in scenario 4a. Testing the geofencing technology was accomplished during the daily operations of the shippers, carriers, and consignees. Since no alerts were generated during normal operations, staged events were used to generate and test the alerting capabilities to the dispatcher, roadside safety enforcement officers, and the PSRC. The test team collected data remotely on usage of this technology and verified the application and use during site test visits at the Illinois weigh station scale just across the border from St. Louis, MO in February, 2004. R&R provided the truck and driver for this event.

During the on-site tests the team successfully observed alerts for out-of-route as well as entering an exclusionary zone/geofence. Alerts came across handheld computers, phones, and pagers successfully.

4.5.11 FR 2.5 Untethered Trailer Notification and Tracking by Dispatcher

This FR required the application of vehicle and tracking technologies that provided the dispatcher the capability to monitor when hazmat trailers were unhooked from the cab and the ability to track the trailers while untethered. The technologies deployed to provide this capability were Qualcomm's QTRACS system and the tethered and untethered trailer tracking technology.

QTRACS – The QTRACS tracking system technology used to address this FR is identical to that described for FR 1.9.

Tethered Trailer Tracking – The TrailerTRACS technology was used to address this FR is identical to that described for FR 1.9.

Untethered Trailer Tracking – Qualcomm provided a derivative of their GlobalTRACS asset tracking system to provide the functionality of untethered trailer tracking. The proof of concept technology provided for the FOT provided real-time trailer identification, connect/disconnect time and location, geo-fencing, unscheduled movement identification capabilities. It utilized a multi-mode terrestrial wireless technology that provided better geographic coverage by limiting blackout and dead spot areas.

The Untethered Trailer Tracking unit used a rectangular geofence area. The area was defined by the latitude and longitude of its center, its east-west width, and its north-south height. When the trailer was connected to the tractor and receiving external power, it continually checked its GPS position. If the trailer was moved into or out of a geofenced area, an alert was generated and sent to the carrier. The unit switched over to its own battery power when disconnected from the tractor and recorded the current GPS position of the trailer. When the carrier received notification of the trailer disconnect from the Tethered Trailer Tracking Unit, he/she sent a message to the Untethered Unit to set the width and height of the geofence. The unit then powered down to save battery power. The unit would reawake when the tractor is reconnected or periodically in the absence of external power. At this time its position was checked. If it had left the geofence area an alert was sent to the carrier.

The untethered trailer tracking technologies were deployed in scenario 4b. Testing this technology was done by remote collection of records from daily activities by the independent evaluation team.

The on-site testing of this technology was not performed with the California Highway Patrol (CHP) due to the seasonal shipments into Lincoln California. No shipments were planned during the active testing period. One reason for this was the irregular demand requirements associated with this shipment. The load was specialized explosives that were only manufactured when Orica placed an order. Unfortunately, no orders were placed by Orica during the operational period. Other factors impacting the seasonality of these shipments related to the route of the shipment. The route included traversing the Donner Pass in western California, which is frequently closed due to severe weather conditions during the winter months.

4.5.12 FR 2.6 Hazmat Cargo Tampering Alert to the Driver and the Dispatcher

This FR required the application of technologies that provided the drivers and dispatchers notification if their hazmat cargo was tampered with.

The technologies implemented to address this FR were identical to those described above for FR 1.5.

4.5.13 FR 2.7 Remote Cargo Locking and Unlocking by the Dispatcher

This FR required the application of technologies that provided the dispatchers the capability to remotely control access to the hazmat cargo.

The technologies implemented to address this FR were identical to those described above for FR 1.6.

4.5.14 FR 2.8 Real-time Emergency Alert Message Notification by the Driver to the Dispatcher

This FR required the application of technologies that provided the drivers with a method of notifying dispatchers of emergency situations.

The technologies implemented to address this functional requirement were wireless (key fob[10]) and dash-mounted panic buttons.

Wireless Panic Button – The wireless panic button (WPB) was a device that could be carried by the driver to remotely send an emergency alert (via satellite or terrestrial communications) and/or to disable the vehicle. There is a separate button for each function on the Wireless Panic Button

[10] Key fob refers to the wireless transmitter hung at the end of a key chain.

Transmitter. The button that is used to send a panic message is recessed to prevent accidental activation.

The process used to test the wireless panic button included:

1. Driver presses red panic button on wireless transmitter.
2. Transmitter sends "panic message" signal to mobile unit.
3. Mobile unit forwards panic message to NMC.
4. NMC forwards panic message to carrier and PSRC and calls carrier and law enforcement with vehicle identification number.

The wireless panic button technologies were deployed in scenarios 1a, 1b, 2a, 3a, 3b, 3c, 4a, and 4b. Testing this technology was accomplished during staged event testing with the independent evaluation team. The test team collected data on usage of this technology and verified the application and use during site test visits on all occasions with Dupre (in conjunction with the Texas Department of Public Safety), Cox (in conjunction with the California Highway Patrol), Distech, Transport Services, Quality, Roeder (in conjunction with the New York State Police), and with R&R (in conjunction with the Illinois State Police).

During the on-site tests simulated panic messages were successfully delivered to the dispatcher, driver manager, public sector reporting center (PSRC), and state agency's dispatch, pager, and hand held computers. Most alerts were delivered within 20 seconds to 2 minutes. The distance from the driver to the cab of the vehicle was approximately 5 feet on the first test and 150 -200 feet on second test.

In-Dash Panic Button – A panic button was mounted inside the vehicle on the dash to send an emergency alert (via satellite or terrestrial communications). For safety purposes, the vehicle can not be disabled with the wired panic button.

The process used to test the in-dash panic button included:

1. Driver presses wired panic button on dash.
2. "Panic message" signal to mobile unit.
3. Mobile unit forwards panic message to NMC.
4. NMC forwards panic message to carrier and PSRC and calls carrier and law enforcement with vehicle identification number.

The in-dash panic button technologies were deployed in scenarios 1a, 1b, 2a, 3a, 3b, 3c, 4a, and 4b. Testing this technology was accomplished during staged event testing with the independent evaluation team. The test team collected data on usage of this technology and verified the application and use during site test visits listed above under wireless panic testing.

During the on-site tests panics were successfully delivered to the dispatcher, driver manager, public sector reporting center (PSRC), and state dispatch, pager, and hand held computers. Most alerts were delivered within 20 seconds to 2 minutes.

4.5.15 FR 2.10 Real-time Emergency Alert Message Notification by the Vehicle to the Dispatcher if Vehicle Senses an Unauthorized Driver

This FR required the application of technologies that sensed when an unauthorized driver was attempting to operate the hazmat vehicle and notified the dispatcher (without the need for driver intervention).

The technologies deployed and the testing protocol to address this FR were the global login and biometric verification technologies described earlier in the description for FR 1.1. After three failed login attempts on either the global login or the biometric verification systems, an alert message is sent to the dispatcher via the NMC of an attempted unauthorized access.

The global login and biometric verification technologies were deployed in scenarios 1a, 1b, 2a, 3a, 3b, 3c, 4a, and 4b. Testing this technology was accomplished during staged event testing with the independent evaluation team. The test team collected data on usage of this technology and verified the application and use during site test visits listed under FR 1.1

During the on-site tests the evaluation team observed successful and unsuccessful login attempts which generated the appropriate alerts. Alerts were verified from visual, electronic records, and state agency receipts of notifications.

4.5.16 FR 2.11 Real-time Emergency Alert Message Notification by the Dispatcher to Local and State Law Enforcement Officials and Emergency Responders

This FR required the application of technologies that provided for real-time notification of local and state law enforcement officials when dispatchers became aware of emergency situations.

The primary technology deployed to address this FR was the PSRC. Whenever an alert message was generated by one of the other technologies (global login, biometric verification, in-dash panic buttons, wireless panic buttons, geofencing alerts), at the same time the message was sent to the dispatcher it was also sent to the PSRC. Using intelligent software, the PSRC would analyze the alert and based on the vehicle, location, and cargo would notify the appropriate law enforcement personnel and carrier dispatch. The notification was done using a variety of communication means including telephone calls, email, fax, and text message. Each law enforcement agency and carrier participant could establish their own custom protocol for who to contact and how when an alert was generated that applied to them. Once these rules were established, the actual implementation of the notification process was automatic through the PSRC process.

The PSRC notification process was deployed and tested in scenarios 1a, 1b, 3c, and 4a. Testing this technology was accomplished during normal daily operations and staged event testing with the independent evaluation team. The test team collected data on usage of this technology and verified the application and use during site test visits with Dupre and the Texas Department of Public Safety in February, 2004, with Cox and the California Highway Patrol in March, 2004, with Roede and the New York State Police in February, 2004, and with R&R and the Illinois State Police in February, 2004.

During the on-site tests the evaluation team observed proper escalation of the alerts. They did observe one problem while testing with CHP and Cox where a redundancy of escalations would have made it successful. This was a good test and gave real world feedback of designing a production alerting system with built-in redundancy.

4.5.17 FR 2.12 Remote Hazmat Vehicle Disabling by the Driver

This FR required the application of technologies that gave the hazmat drivers the capability to remotely (from outside the cab of the truck) disable their vehicle.

The technology deployed to address this FR was the wireless panic button.

Wireless Remote Vehicle Disabling – The driver-initiated vehicle disabling was implemented with a wireless transmitter, carried by the driver, and a wireless receiver, mounted in the vehicle. In an emergency situation, the driver could disable the vehicle by depressing the Aux button on the wireless transmitter. Once the situation was resolved, the driver re-enabled the vehicle by depressing the Test/Reset button. The device complies with part 15 of FCC rules and the range of the transmitter was approximately 150 feet (line of sight).

The wireless remote vehicle disabling technology was deployed in scenarios 1a, 1b, 2a, 3a, 3b, 3c, and 4a. Testing this technology was accomplished during staged event testing with the independent evaluation team. The test team collected data on usage of this technology and verified the application and use during site test visits listed in FR 1.1.

During the on-site tests the evaluation team observed the driver remotely disabling (sending into limp mode) the vehicle from 5 – 400 feet in some cases. The disabling technology was only activated and installed during on site testing with participants and state agencies.

4.5.18 FR 2.13 Remote Hazmat Vehicle Disabling by the Dispatcher

This FR required the application of technologies that gave dispatchers the capability to remotely disable their vehicle.

Remote Vehicle Disabling – An On Board Computer provided the ability to sense and control door locks over the satellite, activate either a siren or headlights and horn of the truck when a security breach was detected and an over-the-air signal could also be sent to notify both dispatch and a remote monitoring location at the host of a problem detected. The unit provided loss of signal detection and response, based upon a programmable configuration of sensed inputs such as speed, time and temperature. The unit is small and easily concealed.

The On-Board Computer (OBC) vehicle disabling system was hosted on a Windows server at the NMC using the QT/Brazil software application. The application provides the ability to configure the OBC, enable/disable the vehicle, and receive cargo lock alerts. When the vehicle disable message is sent, the throttle was reduced to only idle speed so the vehicle can retain power, steering and brakes.

The remote vehicle disabling technology was tested on scenario 1b, 2a, and 4a. Testing this technology was accomplished during staged event testing with the independent evaluation team. The test team collected data on usage of this technology and verified the application and use during site test visits with Cox and the California Highway Patrol in March, 2004 with Distech in December, 2003 and March, 2004, and with R&R and the Illinois State Police in February, 2004.

During the on-site tests the evaluation team observed over-the-air disabling with commands from dispatch as well as loss of signal disabling (simulated by disconnecting the cables). Disable commands effectively reduced the vehicle operation to the limp mode within 20 seconds to 1 minute 20 seconds from the time the command was sent. The required re-enable full operation of the vehicle averaged 30 seconds from the time the command was issued. The loss of signal re-enable commands took approximately 1-2 minutes to take effect after the cables were re-connected.

4.5.19 FR 2.14 Hazmat Driver Identification and Verification by the Vehicle if the Vehicle is Motionless for 10 Minutes

This FR required the application of technologies onboard the vehicle that sensed when it was motionless and required the driver to re-establish authorization any time the vehicle was motionless for more than 10 minutes with engine idling.

The QTRACS vehicle tracking system was configurable to monitor vehicle movement and log off the driver any time the vehicle remained motionless for more than 10 minutes. The process to test driver login was described earlier in FR 1.1.

This FR was tested in scenarios 1a and 1b as part of the global login procedures.

4.5.20 FR 3.1 Remote Cargo Locking and Unlocking by the Dispatcher

Addressing this FR at the receiver's facility was accomplished in an identical fashion to that described earlier for addressing FR 2.7 for en-route applications.

4.5.21 FR 3.2 Hazmat Driver Identification and Verification by the Receiver

Addressing this FR at the receiver's facility was accomplished in an identical fashion to that described earlier for addressing FR 1.1 for shipper applications.

4.5.22 FR 3.3 Hazmat Cargo Verification by the Receiver

Addressing this FR at the receiver's facility was accomplished in an identical fashion to that described earlier for addressing FR 1.2 for shipper applications.

4.5.23 FR 3.4 Receiver Confirmation of Received Cargo to the Driver and Dispatcher

Addressing this FR at the receiver's facility was accomplished in an identical fashion to that described earlier for addressing FR 1.2 for shipper applications.

4.6 Issues Identified and Lessons Learned from the Field Operational Test

Throughout the course of a highly involved, technically sophisticated field test, there are always many unexpected yet highly valuable lessons that can be documented. The Battelle Team was able to witness and document these findings throughout the system installations, data collection, and interaction with system users. If adjustments were feasible and did not compromise the research objectives, they were made with the advance notification of, and approval by, the project sponsor. However, some of the lessons learned came from qualitative interviews with carrier and driver participants and were not easily remedied.

The majority of the documented lessons learned were discovered during the actual FOT through participant usage, interviews, and site visits. The issues identified and lessons learned were generated from the deployment of technologies to address the vulnerabilities from the Task 1 Threat and Vulnerability Assessment report. Only those vulnerabilities that were determined could be addressed by technology solutions were addressed in this FOT. Vulnerabilities that dealt with the physical environment (i.e., need for perimeter fencing), operational issues (such as better sign-in procedures), or environmental issues (i.e., hazmat delivery in close proximity to high-value target) were not addressed in this FOT. The following discoveries are distinguished by each of the technology groupings.

4.6.1 Technology and Operational Issues

Technological interoperability worked well because of the limited project size and scope; however, the many computing platforms used by the numerous data owners in the industry will present a technical challenge for future work of this nature.

Biometrics & Smart Cards

- The biometric fingerprint readers utilized existing hardware not originally intended for a truck cab environment and did not easily conform to ergonomic designs for in-cab telematic systems. As expected, the readers were difficult to properly position in some trucks, and a number of drivers felt the devices interfered with their "space". During the actual installation of the device, it was very hard to position screws due to the small amount of space between the mount and the box. In addition, box cables need to be at least 6 feet long for ease of after-market installation. This issue could be easily rectified by installing the system into the dashboard console, or utilizing a smaller, less obtrusive reader.

- On a positive note, many drivers conveyed their interest and preference for biometrics as a replacement for driver's licenses and other credentials that highlighted personal information such as addresses and social security numbers.

- There were several substantive issues regarding fingerprint usage. Drivers had some difficulty finding the proper location on the readers. This resulted in lost time and increased driver frustration. Location markers or guides on the reader as to where the finger should be placed would be very helpful. In addition, unique driver characteristics must be taken into account. For example, one driver had poor circulation in his right arm and left hand fingerprints had to be used.

- Driver training was critical to the success of biometric reader acceptance, and when drivers were re-trained on the readers, their participation was higher.

- Cold, moist mornings often resulted in added condensation, making the log-in process more difficult. This is a relatively common issue for biometric readers in general with no simple solution. Certain biometric systems work better than others in cold weather; anecdotally, circuit chips perform better than optical readers in this respect.

- Smart cards sometimes fell out of the reader on rough roads. This problem could be easily rectified with design revisions such as improved smart card guides.

- A related issue is that smart cards tend to warp in wallets and pockets, making insertion and placement somewhat more challenging. A strong consideration for future cards is to utilize the contactless cards that are now seeing increased market usage.

- The biometric unit takes 40-45 seconds to turn on after the key has been turned. Drivers felt this was too long.

- Improved usage rates were recorded on dedicated driver runs. If a driver moved to a different vehicle for 2-3 weeks, they did not remember how to use the device. This would not be an issue if the entire corporate fleet were equipped with biometric devices.

- Companies liked the idea of not having to copy their paperwork and DL and just using an automated system; of having a secure personnel ID system; and of having a system for wirelessly transferring and revising cargo data while the vehicle is en route.

Electronic Data Transfer & ESCM

- The Electronic Supply Chain Manifest (ESCM) generated issues similar to those identified in the original U.S. DOT-sponsored FOT in 2001 [8]. These issues typically focus around data transfer issues associated with slow dial-up connections and/or ISP issues. High-speed digital infrastructure such as T1 lines, DSL, and broadband cable generally eliminate ESCM connectivity issues.

- Another problem experienced in both the hazmat and original ESCM FOTs was hardware and software crashes resulting from unauthorized use of the computer for games and web-surfing. The regrettable solution is to eliminate access to the computer's hard drive and CD by removing them.

- Ultimately it is important to integrate an ESCM-like system with other business management systems in order to eliminate the redundancy that comes from multiple and extraneous steps associated with stand-alone systems.

- Improved user name/password match between the ESCM and QTRACS/Global Login could be accomplished through enhanced system integration.

- The company administrators at ESCM sites were occasionally unable to login to the ESCM system. This was attributed to infrequent use, and fingerprint verification issues likely related to fingers misplaced on the readers.

- Frustration arose when participants were occasionally required to process both electronic and paper-based bills of lading. If an ESCM were expanded to a larger-scale application, it is likely that redundant processing would decrease concurrent with a reduction in paper-based transactions.

- While the ESCM software attempted to duplicate paper-based transactions, users proposed improvements to the ESCM user interface.

Mobile Communication Terminals (MCT)

There were fewer issues and concerns with the MCTs (and the related driver interface) since these devices have evolved through many market-generated iterations. While technical issues with the MCTs were nearly non-existent, there were some ergonomic and qualitative comments. (For instance, one qualitative interview with a driver raised the issue of MCT placement in the truck cabs). In one truck fleet, a special bracket held the MCT in place facing rearward (towards the trailer). The driver stated that it was hard to read incoming messages during daylight hours and that it required him to stop and remove the MCT from the bracket.

- Newer generation MTCs only have one external port where older MTCs have 2 ports. These ports were needed by the suite of systems including e-seals, OBCs, and the biometric smart card readers; obviously not all are used at once due to the port limitations. A future port expander will alleviate this issue if multiple technologies are needed on the same vehicle.

Global Login

- Some drivers were irritated by the beeping triggered when someone does not log in. This occurred when drivers refused to log in due to union issues; forgot how to use the system since it had been some time since they had driven vehicles with the technology; had forgotten their smart card; or had other issues.

- One participating carrier had some issues with drivers being bumped off the system after being logged in.

- This feature was heavily used and some drivers preferred it to the biometric verification. Based on driver comments, the research team speculates that this finding results from some combination of (a) greater familiarity with the existing Global Login, (b) privacy concerns associated with biometric readers, and (c) more frequent technical problems with biometrics.

Cargo Door Locking Systems

- Data collection was difficult to manage because the data had to be captured from the carrier's database.

- The door lock was used successfully in day-to-day operations and on-site testing.

- One carrier used a pin in the lock to keep it in the unlocked position so it could be used on trucks without an OBC.

- Time between wireless command to unlock cargo door and its automatic relocking was reconfigured from 20 seconds to 1 minute to provide drivers enough time to move from the truck cab to the trailer door. This amount of time worked well.

E-Seal System

The e-seal devices were used in this FOT as a concept technology. While they have some utilization in other sectors of the freight industry, they are not currently used in the for-hire trucking industry. The primary benefit of e-seals is their ability to provide immediate notification of a security breach or unauthorized access to the hazmat cargo. They are not necessarily a technology designed to prevent specific terrorist incidents.

- For operation and security purposes, some type of indicator is needed to determine when a tag is inoperable.

- E-seals showed some benefits over other approaches. Padlocks were susceptible to key loss and bolts were too difficult to legitimately cut.

- Placement of the antenna allowed it to be too easily damaged and detection of tags was not reliable.

- Drivers removed the handheld from the truck for security purposes which caused battery failure.

- Newer, heavy-duty trailers and trailer doors interfered with the tag's data transmission. The tag vendor indicated that newer versions of the tag would address this issue.

- Even with e-seal training, it was apparent that the system was extremely complex, likely resulting in low driver usage.

- Actual time spent by the driver affixing and managing tags prior to departing is significant. Additional driver comments included "handhelds have an extremely small screen that is not easy to read" and "buttons on the handheld unit are too small".

- E-seal System Reboot Recovery is time consuming and not user-friendly, i.e., resets the handheld configuration at 45 minutes per driver.

- Handhelds are not able to store and forward information.

- There were several occurrences in which the individual managing the e-seal site was unable to communicate with the e-seal application server.

- The notification process was random. Sometimes an e-mail was provided and other times not.

Geofencing

- Geofencing as a concept had extremely high interest by both industry and government, however the technical design needs revisions including improved position resolution and more complex protocols (bases for exceptions, identification and interdiction). From a carrier perspective, this would provide better asset management.

- Initially, some valid user names and passwords were not accepted. The research team rectified this issue.

- One carrier wanted to import electronic routes from the system into it for ease of operation. The user felt it was too time-consuming creating routes manually on the map.

- Another carrier used the display mapping capabilities of geofencing effectively as a tracking technology to reroute trucks around an area in which someone shot at one of their trucks.

Portable Phone with P&D Software

The portable phone was used at only one carrier. User comments included:

- The phone's display is small and may be difficult for older drivers to see; the menu button is very complex, and button navigation is challenging, resulting in correcting and reselecting due to the navigation button design.

- The cellular coverage in the primary area of test, South Louisiana, was not strong off 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. The carrier stated that it is extremely important for them to know where their drivers are at all times; GPS functionality would address this.

- The limited test macros worked well. The test carrier currently uses a more advanced communications system in their over-the-road trucks. If they were to deploy the portable phone instead, they would need the capability to use the same macros and user-defined parameters that are available with their current system.

- Overall, the carrier felt it is a viable commercial solution for medium to large carriers if several key improvements are made, such as larger viewing screen and integration with other management and communication systems.

Panic Buttons

- Although only tested in staged tests and interim visits, many drivers were extremely excited to have both the in-dash and key fob[11] panic button.

- There were 2-3 units at one participating carrier that did not function. This was corrected in a later visit.

- Panic buttons were viewed as "insurance policies"; carriers did not expect to use them, but felt their presence created peace-of-mind for drivers.

Untethered Trailer Tracking

- Several electrical power issues arose and were centered on Pin 7 of the 7-way connector. Many trucks were found to have blown fuses. It was determined that some batteries were drained even when connected. Working with the carrier maintenance team, the issue was ultimately solved.

- One battery was discovered that would not hold a charge. It was located and replaced. However, the new battery also discharged very quickly suggesting other electrical problems with this trailer.

- Several of the 7-way connectors on the trailers were found to be old and corroding. These had to be repaired.

- Trailer tracking in general is getting more attention by industry and government for both security and operational purposes. Given the relatively high number of "misplaced" trailers and shipper requirements to better manage cargo, trailer tracking systems have increased substantially. Security benefits are presently unknown but are being tested by the U.S. DOT in other ongoing field tests.

[11] Key fob refers to the wireless transmitter hung at the end of a key-chain.

Tethered Trailer Tracking

- Installing the tethered trailer tracking fuse on more tractors would have provided more reliable data on this technology. Hook and drop information, sent from dispatch over the satellite system, was only visible on 10 trucks when hitching to the trailer.

Terrestrial Communications

- Terrestrial communication systems are less expensive than satellite systems, possibly making them a preferred system for smaller carriers.

- One carrier conducted an internal operational analysis of its (terrestrial) tracking system, which indicated it provided a positive ROI based on a cost-benefit survey of facility managers and data analysis. Because of the differential cost structure between satellite and terrestrial systems, it is unclear how the ROI could be extrapolated to satellite systems.

Public Sector Reporting Center

There are a number of issues and lessons learned that were identified concerning the integration of public sector agencies into the FOT:

- The PSRC approach, when shown to non-public sector users, was of tremendous interest to them. They saw the value to being provided with proactive messaging to enable them to enhance their safety and security programs.

- Public sector agencies need to have a solution that is exception-based, is simple to use and is reliable at all times. False alarms drain valuable resources and confidence in the system.

- Law enforcement is reluctant to rely on an operational system that is primarily built and managed by the motor carrier industry. The operational mandates of law enforcement and emergency response are different and as a result, the technological systems in use are different. Future work should focus on integrating the PSRC approach with these systems (e.g., computer aided dispatch systems) to provide a value-added service.

- The PSRC infrastructure for the FOT supplemented existing systems and technologies in use by the public agencies involved. Future consideration should be given to the integration of these capabilities with existing public sector devices as well as with future devices.

- The data silo work and exception-based rule alerting was predicated only on the availability of raw data. The approach on the acquisition of source data to feed the data silo was to work with BSG, Qualcomm, and the participating shippers, carriers, and law enforcement agencies to define the data sources and establish agreements under which these data was moved, shared, and used. Many more stakeholders hold data that could enhance the operation and effectiveness of the PSRC. Future consideration should be

given to defining what the optimal, or preferred architecture should be in order to meet ever evolving needs of law enforcement for enhancing hazmat safety and security.

- The field operational test was a vehicle-centric approach, which served well as a baseline. Very little attention was provided during the test to physical or fixed asset infrastructure security. This is important to law enforcement as their mission is not only to protect the moving asset and driver, but also those operating around it and the infrastructure it moves on, through, and around.

- In addition to meeting the research objectives of the FOT, the PSRC was able to demonstrate enhanced, near real-time user functionality including: (a) viewing recent alert notification messages; (b) viewing vehicle and trailer identification data; (c) viewing bill of lading information; (d) viewing carrier, shipper, and consignee contact information; (e) viewing vehicle location data; and (f) sending manual alerts based on driver ID, route adherence, and emergency alert.

- The public sector FOT was not performed in a manner conducive to typical law enforcement operations. The public sector testing was primarily done at carrier terminal locations, which is not an accurate representation of the operational requirements of law enforcement. Further exploration is needed on how to integrate these capabilities/ functions into current operational and technology "protocols" for law enforcement agencies.

- Since PSRC testing was done to minimize the impacts on revenue trips by the participating motor carriers, it was difficult to schedule tests. This led to minimal testing with law enforcement. More frequent and robust testing with law enforcement and emergency response personnel in an operational setting would be beneficial.

- It is difficult to create a joint public-private field operational test that appropriately balances the potential negative operational impacts on either group.

- The public sector testing did not include the incorporation of any law enforcement-sensitive data such as terrorist watch lists, criminal databases, state systems, and other data sources relevant to criminal and security activity. This is something that should be explored for future work of this nature.

- The various types, reliability, security, and cost-effectiveness of communications technologies as they relate to law enforcement was not investigated. In addition, there is a need to investigate the issue of message priority amongst such communications technologies. Alerts relevant to safety and security breaches must take priority over other types of communications.

- Liability concerns need to be identified and defined in terms of when officers become aware of threats/events whether action or inaction presents any potential concerns. This is especially true concerning information coming from non-law enforcement sources.

- The management needs of the data silo, including at what point data should be purged or archived and what events must be logged was not specifically addressed in this operational test. This is an important step in moving ahead with additional work of this nature.

- Law enforcement saw the value of incorporating additional data into the alerts. As such, future work needs to explore the impacts of sending additional data through the modular connector in the data silo for processing and generating alerts. Such information could include more specific vehicle information (e.g., color, markings, description), driver and carrier identification, additional response resources, chemical information, shipper information, population demographics, weather event data, building/structural floor plans, populated places, location of schools, hospitals, major event venues, and even water supplies.

- In order to provide an appropriate environment for operational testing, exception-based agent analysis and message delivery, and queries from law enforcement and first responders, it is critical to have a robust, standardized, central location for all data storage and/or assimilation. Equally as important is having the appropriate interfaces to the data systems that hold the "authoritative" source data.

5.0 Findings and Next Steps

The following section presents the Battelle team's findings and recommendations for "next steps." While the discussion previously in Section 4.6 focused on specific technology and operational issues and lessons learned, this section takes a broader, more macro-observation of the findings of the deployment team and translates those into what the team believes should be considered (at the macro/national level) for future consideration by the U.S. DOT.

5.1 Hazardous Materials Industry

The hazmat industry participants in the FOT were selected by the Battelle Team as being representative of those companies involved with the hazmat shipment categories identified as being of higher concern in the threat and vulnerability assessment. Participating hazmat carriers are categorized in Table 16 below:

Table 16. FOT Carrier Size and Commodity Characteristics

Carrier	Sector	Size (Annual Revenues)	Hazmat Grouping
1: Dupre Transport	Tank	$65,525,630	Bulk Fuel
2: Cox Petroleum	Tank	$21,296,620	Bulk Fuel
3: Distribution Tech	LTL	NA*	LTL High Hazard
4: Roadway Express	LTL	$2,671,185,850	LTL High Hazard
5: Transport Service	Tank	$74,413,700	Bulk Other
6: Roeder Cartage	Tank	$9,036,200	Bulk Other
7: Quality Distribution	Tank	$579,610,000	Bulk Other
8: R&R Trucking	Tank	$48,132,000	Bulk Other
9: Dyno Transportation	Truckload	$13,587,723	Truckload Explosives

*NA: Not available

In addition, the state agencies offered a diverse mix of agency types, sizes, and geographic location. These agencies were the California Highway Patrol, the Illinois State Police, the New York State Police, and the Texas Department of Public Safety.

Even with the broad representation of participants in the FOT, it was very limited in size and scope. There are many more stakeholders (public and private) that could be involved in future projects of this nature.

5.2 Technology Issues and Opportunities

The technologies selected for the FOT can be readily plotted on myriad continuums, such as:

- Level of market usage and acceptance (commonly to rarely used)
- Unit costs (low to high)
- Management costs (low to high)
- Ease-of-use (easy to challenging)
- Technology sophistication (simple to complex; low-tech to high-tech)

While none of the technologies tested would be described as prototypes, several have very limited prior field usage outside of government applications. For example, the vehicle disabling technology is not currently a commercially available product in the United States. However, it is commercially available in other countries such as Brazil. In Brazil, the primary use for this technology has been to stop or deter theft (either of the product or the entire vehicle). The legal climate in Brazil is more conducive (than that of the United States) to the implementation of such technologies at this time. Nevertheless, all the technologies represent the most logical technology application for the particular threat and vulnerability based on a series of research studies and field tests. These technologies are categorized by focus area in Table 17.

Table 17. Technologies by Focus Area

Focus	Management System
Personnel	Biometric verification
Vehicles	Wireless tracking and management
Cargo	Electronic trailer seals Remote door locks Electronic data management

At a high level, most of the tested technologies were well accepted by system users. In some cases, this was based on an existing understanding and familiarity with a common marketplace system such as wireless vehicle tracking. With other systems such as biometrics, there was an acceptance that national security issues and programs (e.g., U.S. Patriot Act) made biometrics an inevitable reality.

Based on qualitative research, it was extremely evident that different stakeholders within the FOT had different perspectives according to their roles; opinions differed across technology investment decision makers, day-to-day users, government regulators, and technology vendors. For example, electronic seals seemed to have higher acceptance among carrier management than among drivers.

5.2.1 Biometrics

The use of fingerprints as an ID system was generally accepted from a security and policy perspective. Nevertheless, biometric system design issues quickly caused driver frustration and backlash. This should not be entirely surprising given that biometric usage in the transportation sector is nearly non-existent. Considerably more resources and testing are needed to ensure that biometrics are designed and applied in a logical and functional manner.

5.2.2 Wireless Vehicle Tracking and Communications

The trucking industry has a long history with wireless vehicle communications and asset tracking, making this component of the FOT one of the most accepted and entrenched of the applied technologies. The technical merits and characteristics of the different technologies that make up this grouping are well understood.

Satellite systems, which include GPS, voice and text communications, and other satellite-based functionalities, presently require good satellite coverage and the well known "line-of-sight" condition (i.e., to be effective, they cannot be blocked by thick vegetation, tall buildings, or tunnels). Therefore, vehicles can lose satellite signals in urban areas, underpasses, and, more rarely, areas with a gap in satellite coverage. From a security standpoint, solutions to this inherent problem are challenging since a conservative policy would be to initiate some action whenever there is a loss of signal. An evolving solution is to utilize hybrid systems that automatically switch between satellites and terrestrial systems based on signal strength and availability.

Terrestrial systems also have technology-based limitations such as gaps in signal coverage in lower density areas, signal interference, and proprietary/interoperability system issues.

5.2.3 Cargo Management

There were several different systems tested in the FOT that focused on identifying and/or protecting the cargo and trailer. Intuitively, these seem to be the most effective and immediate approach since the hazmat cargo itself is the primary concern from a terrorism standpoint. It is interesting that these systems are the least developed and tested of all the systems, at least within the trucking industry.

Electronic seals have received considerable attention over the last few years, with many of the proposed benefits derived from military applications. However, outside of limited U.S. DOT tests, wireless e-seals have little to no presence in the private sector transportation industry. One reason may be the complexity and variability of the seals themselves; almost without exception, each seal is based on a different proprietary system and/or "standard" making integration and interoperability nearly impossible across different e-seal systems.

The second issue is cost. The lower-cost disposable seals typically cost between $3 and $15 per seal. Even in a truckload environment where cargo access is less frequent, it is likely that several seals would be required every day for each truck. If cargo security inspections at weigh stations

and border crossings were to increase as expected, the value of disposable seals would be further eroded.

The alternative is the reusable e-seal, one of which was tested in the FOT. Outside of common issues generally associated with wireless devices (e.g., loss of signal, power management issues, user-friendliness), the primary concern with reusable seals is their high unit cost. While the seal itself may only cost $30 to $50, the requisite support system (e.g., seal readers), typically raises the cost into the hundreds of dollars per truck. With well-documented operating margins of less than five percent, the trucking industry would be hard-pressed to outfit the three million plus trailers that operate on the U.S. transportation system.

5.2.4 Trailer Locks

Electronic trailer locks show some promise from a qualitative user standpoint since cargo theft continues to be a leading problem for the trucking industry. But surprisingly, the Technology Compendium discussed in Section 2.3 and Appendix C indicates that electronic trailer locks are not well established in the industry. Dramatically different trailer configurations along with cost issues can be cited as a likely explanation.

5.2.5 Electronic Freight Data

The Electronic Supply Chain Manifest provided the FOT participants with advanced encrypted hazmat cargo data, which, in theory, should enhance security and cargo management functionality. Participants generally agreed that supply chain management systems are essential, but without tangible efficiency gains from the ESCM system, usage was limited. One potential reason for the limited ESCM usage is that the companies recruited for the FOT did not have frequent runs. Government stakeholders, on the other hand, are beginning to require advance submission of electronic freight data, thus ensuring that some variation of an ESCM system will continue. For example, the Department of Homeland Security (DHS) through U.S. Customs is requiring a 4-hour advance notice for incoming international cargo shipments and the FHWA is in the early stages of developing an electronic freight manifest project to look at potential efficiencies and security enhancements of an international in-bound air cargo electronic freight manifest system. Future iterations ought to expand the efficiency benefits through new services and functionality and improve systems integration so full supply chain management benefits are realized.

5.2.6 Exception-Based Testing

To counter a likely scenario that a terrorist would interfere with some aspect of the vehicle tracking system, a loss-of-signal component was designed and tested. While it generally worked within the logical parameters designed by the research team, for the reasons cited in Section 5.3.2 (primarily non-terrorist/system-based issues), more sophisticated designs and technical parameters are probably necessary.

5.2.7 Geofencing

Two variations of geofencing were tested, best described as out-of-route alerts and critical infrastructure approach. The functional difference between the two is where the circle of influence and notification lays—either with the mobile vehicle or with the static infrastructure. The basic functionality shows promise beyond the obvious security applications. Integration with carriers' existing route planning systems would dramatically improve the utility of geofencing.

5.2.8 Trailer Tracking

Two variations of trailer tracking were tested, tethered and untethered. Prior to 9/11, theft was one of the biggest issues facing the industry. Tethered trailer tracking provided valid hook and drop data points to dispatchers via satellite.

Untethered trailer tracking, currently used on heavy equipment, was also tested as a concept technology. This again utilized satellite communications to the dispatcher but allows the trailer to communicate even when separated from the tractor. This provides visibility of the trailer at all times. Trailer tracking provides critical information about the location and status of the cargo that can be used to identify potential security violations.

5.3 Data Privacy Issues

It must be pointed out that various non-disclosure agreements were developed and signed as part of the FOT. This is indicative of the sensitive nature of information which included proprietary technology information, competitive operating data, and concerns about government access and use of private sector data and processes.

This issue will become more prominent as new government programs and systems require more data input and manipulation, and the private sector becomes more sensitive to the new disclosure demands. One opportunity for resolving these issues may lie with the FHWA Freight Information Highway initiative which, among other things, is attempting to develop new data-sharing agreements and partnerships between business and government.

5.4 Summary of Findings

The Battelle Team identified a number of key findings:

- Personnel expectations differ by roles and responsibilities. All stakeholder levels must be managed and trained, taking into account each group's expectations and perspectives.
- Technologies must meet the financial requirements of freight industry investors and decision makers and the ease-of-use needs of drivers and attendants.

- Multifunctional security technologies would promote higher system usage by the trucking industry.

- To support national security policies and programs, technology vendors should work together to focus on standardization of data and systems with an ultimate goal of system interoperability and/or data interchanges.

- Differing public- and private-sector expectations for returns on safety and security initiatives support the premise that costs and benefits should be determined and assigned to different beneficiaries. Carrier benefit costs should be borne by industry; societal benefit costs should be borne by society.

6.0 References

1. U.S. Census Bureau, 1997 Vehicle Inventory and Use Survey (VIUS).

2. Battelle, *Hazmat Safety and Security Field Operational Test Task 1: Risk/Threat Assessment*, Federal Motor Carrier Safety Administration, December 4, 2002.

3. Battelle, *Comparative Risks of Hazardous Materials and Non-hazardous Materials Truck Shipment Accidents/Incidents: Final Report*, Federal Motor Carrier Safety Administration, March 2001.

4. Battelle, *Hazmat Safety and Security Field Operational Test Task 4: System Requirements and Design*, Federal Motor Carrier Safety Administration, July 17, 2003.

5. Battelle, *Hazmat Safety and Security Field Operational Test Task 4: Public Sector System Requirements and Design*, Federal Motor Carrier Safety Administration, December 17, 2003.

6. Battelle, *Hazmat Safety and Security Field Operational Test Task 2: Concept of Operations*, Federal Motor Carrier Safety Administration, April 18, 2003.

7. Battelle, *Hazmat Safety and Security Field Operational Test Task 2: Public Sector Concept of Operations*, Federal Motor Carrier Safety Administration, November 11, 2003.

8. American Transportation Research Institute. *Phase II: Developing and Testing an Electronic Supply Chain Manifest*, Federal Aviation Administration and Federal Highway Administration, December 2002.

Appendix A.
Detailed Scenario Descriptions

Introduction

The detailed scenario descriptions look in depth at all four scenarios and act as a reference to this document. Additional information can be found in the Concept of Operations document. Information for each scenario included the following:

- Hazmat class description, as well as route and delivery information
- Participant information of shippers, trucking companies and consignees
- Technologies tested by truck
- FOT operational information.

In addition to the above information, details on the public sector reporting center are also listed within the scenario descriptions.

A.1 Scenario 1 – Bulk Fuel Delivery

Dupre Transport (1a) provided 13 short haul fuel delivery vehicles, delivering Class 3 (Flammable Liquids). Deliveries were made in roughly a 100 mile radius of Houston, TX, Dallas, TX., San Antonio, TX., and Austin, TX. The technologies installed per truck are listed later in Table A-1.

Scenario (1b) with Cox Petroleum provided 12 short haul fuel delivery vehicles, delivering Class 3 (Flammable Liquids) in the southern and central California region ranging from San Diego north through the Bay Area to Sacramento on the north. The technologies installed per truck are listed later in Table A-2.

A.1.1 Participants

Scenario	Vehicles	Shipper	Carrier	Consignee	Public Sector Agencies
1a	13	ExxonMobil	Dupre Transport	Various	Texas Department of Public Safety
1b	12	ExxonMobil	Cox Petroleum	Various	California Highway Patrol

ExxonMobil markets gasoline and other fuels at almost 43,000 service stations in 118 countries and has over one million industrial and wholesale customers around the globe. The company has aviation facilities in more than 700 airports in 80 countries. ExxonMobil Marine Fuels serves more than 300 ports in 70 countries.

Dupre Transport, headquartered in Lafayette, LA, provides both bulk tank and dry van services to a variety of customers in the petrochemical industry. Typical products hauled by the bulk tank

group include; gasoline, diesel, aviation fuels, crude oil, liquefied petroleum gas, and various types of petrochemicals. The company operates over 250 company-owned tractors within a network of approximately 25 terminal locations. Primary areas of operation are Texas, Louisiana, Arkansas, Tennessee, Mississippi, and Alabama, but range as far as Florida, Minnesota, and New York.

Cox Petroleum Transport is a common carrier trucking company specializing in petroleum product transportation. It services the California market, hauling gasoline, diesel fuel, jet fuel, lube oils, crude oil, and fuel oils. Cox has eight terminals located throughout Central and Southern California. Leading customers include ARCO, Exxon Mobil and Chevron.

Texas Department of Public Safety (DPS) for Dupre and the **California Highway Patrol** (CHP) for Cox tested state agency support.

Tested Technologies

The following technologies were tested in this scenario:

- Wireless Satellite Communications (w/GPS)
- Wireless Terrestrial Communications handheld w/pickup and delivery (P & D) software
- Driver Authentication with Global Login
- Intelligent Onboard Computers (OBC)
    - Wireless Vehicle Disabling
- Panic Button in Dash
- Panic Button Wireless/remote
    - Remote Vehicle Disabling
    - Remote Emergency Notification

A.1.2 Technologies by Truck

Tables A-1 and A-2 present the specific technologies that were installed on each of the 25 trucks that were tested in this scenario. The suite of technologies are mapped to the technology tier described earlier as well as the functional requirements that was addressed.

A.1.3 Operational Description of Scenario

Cox and Dupre had used the satellite system extensively before and during the actual FOT. They both use the system for positioning, daily messaging, and operations. Terrestrial communications were added to Cox and digital phones to Dupre to see how they would perform in the fuel delivery market.

Table A-1. Technologies per Truck on Scenario (1a)

Truck	Technologies				Tier	Shipper	Carrier	Functional Requirements
1	Satellite Comm.	Panic Dash/WPB	Global Login	WVD	T-3	Exxon	Dupre	1.1,1.3,1.4, 2.1-2.3,2.8,2.10,2.11,2.14,3.4
2	Satellite Comm.	Panic Dash/WPB	Global Login	WVD	T-3	Exxon	Dupre	
3	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
4	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
5	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
6	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
7	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
8	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
9	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
10	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
11	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
12	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	
13	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Dupre	

Table A-2. Technologies per Truck on Scenario (1b)

Truck	Technologies				Tier	Shipper	Carrier	Functional Requirements
14	Satellite Comm.	Panic Dash	Global Login	OBC	T-4	Exxon	Cox	1.1,1.3,1.4, 2.1-2.3,2.8,2.10,2.11,2.13,2.14,3.4
15	Satellite Comm.	Panic Dash	Global Login	OBC	T-4	Exxon	Cox	
16	Satellite Comm.	Panic Dash	Global Login	OBC	T-4	Exxon	Cox	
17	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Cox	1.1,1.3,1.4, 2.1-2.3,2.8,2.10,2.11,2.14,3.4
18	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Cox	
19	Satellite Comm.	Panic Dash	Global Login		T-3	Exxon	Cox	
20	Satellite Comm.	Panic Dash/ WPB	Global Login	WVD	T-3	Exxon	Cox	
21	Satellite Comm.	Panic Dash/ WPB	Global Login	WVD	T-3	Exxon	Cox	2.3,2.12,
22	Satellite Comm.	Panic Dash/ WPB	Global Login	WVD	T-3	Exxon	Cox	
23	Satellite Comm.	Panic Dash/ WPB	Global Login	WVD	T-3	Exxon	Cox	
24	Terrestrial Comm	Panic Dash			T-2	Exxon	Cox	
25	Terrestrial Comm	Panic Dash			T-2	Exxon	Cox	

Driver identification was performed with the Global Login feature that was new to both operations. The drivers had to login their username and password after each time the truck was started or had been disabled. This proved to be extensive in this operation.

Both carriers also had wired and wireless panic buttons installed in their tractors. The panic buttons were only used during on-site evaluations with the evaluators and during public agency testing with Texas DPS and California CHP. The Wireless Vehicle Disable (WVD) was also used during these controlled tests with the state agencies and evaluators in a controlled environment to disable the throttle of the tractor.

Lastly, Cox had onboard computers (OBC) installed on their tractors. The functionality of these OBC's for loss of signal disabling, and OTA disabling were tested on site at Cox in a controlled environment during CHP and evaluation testing.

A.2 Scenario 2 – LTL High Hazard

Scenario (2a) with Distribution Technologies involved 12 dedicated high hazard "LTL-like" type of vehicles. These vehicles are tanks with segregated partitions which carry up to seven different types of chemicals/hazards entailing seven stops per trip. Vehicles were dispatched out of Macon Georgia, and cover various southeast U.S. locations. The actual technologies installed per truck are listed later in Table A-3.

Scenario (2b) with Roadway Express involved 13 LTL Pick up and Delivery (P&D) type of vehicles. This part of the FOT monitored a lower cost (terrestrial hardware) technology installed on a national LTL fleet with a very high degree of integration and efficiencies. These trucks are dedicated for local P&D operations, usually without a dedicated driver, route or truck. The trucks provided were based out of San Diego, California, for the purposes of this test. The technologies that were installed per truck are listed later in Table A-4.

A.2.1 Participants

Scenario	Vehicles	Shipper	Carrier	Consignee	Public Sector Agencies
2a	12	GE Betz	Distribution Technologies (DisTech)	Various	None
2b	13	GE Betz	Roadway Express	Various	None

GE Betz is a global business with offices in more than 50 countries and operations throughout the world. It has four regional centers and 20 production plants located in North and South America, Asia-Pacific, Europe, and Latin America. GE Betz has approximately 3800 employees worldwide.

All former Hercules plants were acquired by GE Betz. The Hercules Macon Georgia plant also manufactures products for GE Betz.

Distribution Technologies is a provider of transportation, distribution, logistics, and supply chain management services through a combination of asset and non-asset based solutions.

Deliveries include DOE processing plants, power generating plants (both fossil fuel and nuclear), sensitive chemical production/distribution facilities, essential medical and health science facilities, municipal water treatment facilities, and ramp areas of military and commercial airports.

Roadway Express is a leading less-than-truckload (LTL) transporter of industrial, commercial, and retail goods in the two- to five-day regional and long-haul markets. Roadway Express provides service between all 50 states, Canada, Mexico, and Puerto Rico with international freight services for 140 countries. Roadway Express specializes in limited load deliveries in which a trailer usually contains cargo from several customers.

Technologies Tested

The following technologies were tested in this scenario.

- Wireless Satellite Communications (w/GPS)
- Wireless Terrestrial Communications
- Driver Authentication with Global Login
- Intelligent Onboard Computers (OBC)
    - Wireless Vehicle Disabling
- Panic Button in Dash
- Panic Button Wireless/Remote
    - Remote Vehicle Disabling
    - Remote Emergency Notification

A.2.2 Technologies by Truck

Tables A-3 and A-4 present the specific technologies that were installed on each of the 25 trucks that will be tested in this scenario. The suite of technologies are mapped to the technology tier described earlier as well as the functional requirements that were addressed.

Table A-3. Technologies per Truck on Scenario 2a

Truck	Technologies				Tier	Shipper	Carrier	Functional Requirements
26	Satellite Comm.	Panic Dash/WPB	Global Login		T-3	GE Betz	DisTech	1.3,1.4,2.1,2.3,2.8,2.10,2.11,2.14
27	Satellite Comm.	Panic Dash/WPB	Global Login		T-3	GE Betz	DisTech	
28	Satellite Comm.	Panic Dash/WPB	Global Login		T-3	GE Betz	DisTech	
29	Satellite Comm.	Panic Dash/WPB	Global Login	WVD	T-3	GE Betz	DisTech	
30	Satellite Comm.	Panic Dash	Global Login		T-3	GE Betz	DisTech	
31	Satellite Comm.	Panic Dash	Global Login		T-3	GE Betz	DisTech	
32	Satellite Comm.	Panic Dash	Global Login	OBC	T-4	GE Betz	DisTech	1.3,1.4,1.6,2.1,2.3,2.7,2.8,2.10,2.11, 2.13,2.14,3.1
33	Satellite Comm.	Panic Dash	Global Login		T-3	GE Betz	DisTech	1.3,1.4, 2.1, 2.3, 2.8, 2.10, 2.11, 2.14
34	Satellite Comm.	Panic Dash	Global Login		T-3	GE Betz	DisTech	
35	Satellite Comm.	Panic Dash	Global Login		T-3	GE Betz	DisTech	
36	Satellite Comm.	Panic Dash	Global Login		T-3	GE Betz	DisTech	
37	Satellite Comm.	Panic Dash	Global Login		T-3	GE Betz	DisTech	

Table A-4. Technologies per Truck on Scenario 2b

Truck	Technologies				Tier	Shipper	Carrier	Functional Requirements
38	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	2.3, 2.8, 2.11
39	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
40	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
41	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
42	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
43	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
44	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
45	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
46	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
47	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
48	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
49	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	
50	Terrestrial Comm	Panic Dash			T-2	Multiple	Roadway	

A.2.3 Operational Description of Scenario

Distribution Technology (DisTech) had used the satellite system extensively before and during the actual FOT. Roadway Express had used the terrestrial system extensively before the FOT but not in the new market of San Diego California. They both use the system for positioning, daily messaging, and operations.

Driver identification was performed with the Global Login feature for DisTech only in this scenario. The drivers had to login their username and password after each time the tractor was started or had been disabled.

DisTech also had wired and wireless panic buttons installed in their tractors. The panic buttons were only used during on site evaluations with the evaluators. The Wireless Vehicle Disable (WVD) was also used during these controlled tests with the evaluators in a controlled environment to disable the throttle of the tractor.

Lastly, DisTech had onboard computers (OBC) installed on their tractors. The functionality of these OBC's for loss of signal disabling, and OTA disabling were tested on site at DisTech in a controlled environment during the evaluation testing.

A.3 Scenario 3 – Bulk Other

Scenario (3a) with Transport Services involved 12 bulk chemical delivery vehicles, delivering hazmat Classes 9, 2, and 4, and D Ester. Routes originated in Midland Michigan and delivered to consignees in Illinois, Missouri, Indiana, and Ohio. The technologies installed per truck are listed later in Table A-5.

Scenario (3b) with (carrier) Quality Distribution involved seven bulk chemical delivery vehicles, delivering Class 3, Flammable, Class 2.2 Non-Flammable with an inhalation hazard. Routes originated in Lima Ohio and have consignees in Kentucky, Tennessee, Arkansas, and Texas. The technologies installed per truck are listed later in Table A-6.

Scenario (3c) with (carrier) Roeder Cartage involved six bulk chemical delivery vehicles, delivering Acrylonitrile (AN), a Class 3, Flammable and Poisonous. Routes originated in Lima, Ohio and had consignees in Illinois and New York. The technologies installed per truck are listed later in Table A-7.

A.3.1 Participants

Scenario	Vehicles	Shipper	Carrier	Consignee	Public Sector Agencies
3a	12	DOW Chemical	Transport Service	NuFarm Americas	Illinois State Police
3b	7	BP Chemical	Quality Distribution	None	None
3c	6	BP Chemical	Roeder Cartage	Evans Chemical	New York State Police

Dow Chemical is a leading science and technology company that provides innovative chemical, plastic, and agricultural products and services to many essential consumer markets. With annual sales of $28 billion, Dow serves customers in more than 170 countries and a wide range of markets that are vital to human progress, including food, transportation, health and medicine, personal and home care, and building and construction, among others. Dow has approximately 50,000 employees worldwide.

Transport Service is based in Hinsdale, IL and is the 16th largest tank truck carrier in the United States. It is also one of the leading independent tank truck carriers of sweetener products. TSC conducts its business through two separate divisions, Chemical and Food Grade. The Chemical Division provides tank truck carrier services to chemical manufacturers from seven terminals, while the Food Grade division focuses on serving manufacturers of bulk liquid food products from four terminals and five satellite locations.

NuFarm Americas was the consignee for Transport Services was in Chicago Heights, IL.

BP Chemical is the world's third largest petrochemicals company, based on a diverse, highly integrated product portfolio in North America, Europe, and Asia-Pacific. BP Chemical manufactures and markets over 25 million tons of petrochemicals, intermediates, plastics, and specialties each year.

The BP Nitriles Business Unit's Lima facility is a major producer of industrial and agricultural chemical products and employees approximately 480 people. Their primary products include acrylonitrile, butanediol (BDO), Barex, and nitrogen. The Lima facility is one of BP Chemical's largest plant sites.

BP Chemical was the dedicated shipper for scenario 3b and 3c. They supplied both product and consignees to carriers Quality Distribution and Roeder Cartage.

Quality Distribution is the largest liquid bulk transportation company in the North American continent. Quality Carriers, Inc, is a subsidiary of Quality Distribution, Inc. Headquartered in Tampa, Florida, Quality Distribution operates approximately 3,400 tractors and 7,900 trailers through principal transportation subsidiaries: Quality Carriers, TransPlastics, and Quebec-based Levy Transport. Quality Distribution also holds varied business interests in other bulk transportation services, including tank cleaning and freight brokerage.

The Quality Distribution terminal in Lima, OH, is mostly dedicated to hauling loads for BP Chemical. There were no consignees involved in testing this scenario. **Eli Lily** as designated consignee, was unable to accommodate this test at the last moment.

Roeder Cartage, Inc. is based in Lima, OH and is a dedicated carrier for BP Chemical.

Roeder Cartage is a participant that has not adopted any vehicle communications technology. They were selected as the only "non-technology adopter" to participate in the FOT.

Evans Chemical of Waterloo, NY was the consignee in this scenario. Onsite state agency testing and evaluations were performed at the Evans facility.

New York State Police was the State agency support.

Technologies Tested

The following technologies that were tested in this scenario:

- Wireless Satellite Communications (w/GPS)
- Driver Authentication with Biometrics and Smart Cards
- Electronic Supply Chain Manifest (ESCM)
- Panic Button in Dash
- Panic Button Wireless/remote
    - Remote Vehicle Disabling
    - Remote Emergency Notification

A.3.2 Technologies by Truck

Tables A-5, A-6, and A-7 present the specific technologies that were installed on each of the 25 trucks that were tested in this scenario. The suite of technologies are mapped to the technology tier described earlier as well as the functional requirements that were addressed.

Table A-5. Technologies per Truck on Scenario 3a

Truck	Technologies				Tier	Shipper	Carrier	Functional Requirements
51	Satellite Comm.	Panic Dash/WPB/WVD	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	1.1-1.4,2.1-2.3,,2.8,2.10-2.12,2.14,,3.2-3.4
52	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
53	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
54	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
55	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
56	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
57	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
58	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
59	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
60	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
61	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	
62	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	Dow	Transport Service	

Table A-6. Technologies per Truck on Scenario 3b

Truck	Technologies				Tier	Shipper	Carrier	Functional Requirements
63	Satellite Comm.	Panic Dash/WPB/WVD	Biometric Auth.	E-Manifest	T-4	BP	Quality Distribution	1.1-1.4,2.1-2.3,,2.8,2.10-2.12,2.14,,3.2-3.4
64	Satellite Comm.	Panic Dash/WPB/WVD	Biometric Auth.	E-Manifest	T-4	BP	Quality Distribution	
65	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Quality Distribution	
66	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Quality Distribution	
67	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Quality Distribution	
68	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Quality Distribution	
69	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Quality Distribution	

Table A-7. Technologies per Truck on Scenario 3c

Truck	Technologies				Tier	Shipper	Carrier	Functional Requirements
70	Satellite Comm.	Panic Dash/WPB/WVD	Biometric Auth.	E-Manifest	T-4	BP	Roeder Cartage	1.1-1.4,2.1-2.3,,2.8,2.10-2.12,2.14,,3.2-3.4
71	Satellite Comm.	Panic Dash/WPB/WVD	Biometric Auth.	E-Manifest	T-4	BP	Roeder Cartage	
72	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Roeder Cartage	
73	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Roeder Cartage	
74	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Roeder Cartage	
75	Satellite Comm.	Panic Dash/WPB	Biometric Auth.	E-Manifest	T-4	BP	Roeder Cartage	

A.3.3 Operational Description of Scenario

Transport Services and Quality Services had used the satellite system extensively before and during the actual FOT. They both use the system for positioning, daily messaging, and operations. Roeder Cartage was a new user of the satellite system for the purposes of this FOT.

Driver identification was performed with the Biometric Login feature for all participants in this scenario. The drivers had to login using their fingerprint and smartcard after each time the tractor was started or had been disabled.

All three carriers had wired and wireless panic buttons installed in their tractors. The panic buttons were only used during on site evaluations with the evaluators. The Wireless Vehicle Disable (WVD) was also used during these controlled tests with the evaluators in a controlled environment to disable the throttle of the tractor.

All trucks in this scenario also had the ability to perform electronic manifest. Dow utilized it with Transport Services shipping product to Nufarm in Illinois. BP utilized it with Roeder Cartage on runs to Evans Chemical in Waterloo. BP was not able to utilize it with Quality due to consignee Eli Lily being unable to accommodate this test at the last moment.

A.4 Scenario 4 – Truckload Explosives

Scenario 4a with R&R Trucking involved 12 truckload explosive delivery vehicles, delivering Class 1.1 – 1.6, Explosives. The loads were delivered using dedicated trucks with dedicated routes. The routes are based out of Charlestown, Indiana (or Augusta GA in the summer) with deliveries in New York, New Jersey, and Illinois. Other routes are based out of Joplin Missouri with deliveries into three cities within Texas. The technologies installed per truck are listed later in Table A-8.

Scenario 4b with Dyno Transportation involved 13 truckload explosive delivery vehicles, delivering Class 1.1 - 1.6, Explosives. The routes were based out of Joplin Missouri with deliveries in New York, New Jersey, and Illinois. The technologies installed per truck are listed later in Table A-9.

A.4.1 Participants

Scenario	Vehicles	Shipper	Carrier	Consignee	Public Sector Agencies
4a	12	Orica USA	R&R Trucking	Orica USA	Illinois State Police
4b	13	Dyno Nobel	Dyno Transportation	Orica USA	California Highway Patrol

Orica USA is the world's leading supplier of commercial explosives and blasting technology. It is a publicly-owned Australian chemical company employing approximately 8,000 personnel in 35 countries. The company's operations are divided into four main business areas – Mining Services, Chemicals, Consumer Products, and Agricultural Chemicals.

The company's main markets are the mining, quarrying, and construction industries. Its product range are divided into broad segments such as initiating systems, ammonium nitrate, bulk explosives, packaged explosives, and blasting services.

Orica USA was the shipper in 4a as well as the consignee on products flowing into their facility from Dyno.

R&R Trucking was established in 1988 as a munitions carrier for the U.S. government. Its main function was to handle dedicated runs for the Department of Defense (DoD). In 1997, R&R Trucking was approved by DOE to transport radioactive materials.

R&R companies specialize in the over-the-road transportation of military munitions, commercial explosives, and radioactive materials. R&R has 15 terminals located across the United States, with its corporate location near Joplin, MO where centralized dispatch is performed. Over-the-road shipments of commercial explosives are typically delivered to blasting sites and bin storage.

Dyno Nobel is one of the world's leading manufacturers of commercial explosives and initiation systems. Dyno Nobel is organized into four business areas: Dyno Nobel America (DNNA), Dyno Nobel Asia Pacific (DNAP), Dyno Nobel Europe (DNE), and the newly formed Dyno Nobel Latin America (DNLA).

Dyno Nobel is the only U.S. manufacturing location for nitroglycerin dynamites. It also produces emulsions and slurries. The manufacturing plant, which employs about 270 people, is located three miles southwest of Carthage, MO.

Dyno Nobel Transportation, Inc. is the private fleet transportation service for Dyno Nobel which operates a manufacturing facility directly across the street in Carthage, MO. Dyno Nobel Transportation primarily transports Class 1.1 through 1.5 explosives, and detonator shipments, originating in Carthage, MO throughout the United States and Canada.

Dyno of Lincoln, California was the consignee originally set up for this test. This run was extremely limited due to seasonal loads and planning.

State agency support was tested with **Illinois State Police** for R&R trucking.

Technologies Tested

The following provides the technologies that were tested in this scenario.

- Wireless Satellite Communications (w/GPS)
- Driver Authentication with Biometrics and Smart Cards
- Electronic Supply Chain Manifest (ESCM)

- Intelligent Onboard Computers (OBC)
    - Remote Vehicle Disabling Dispatcher or Parameter Set
    - Remote Lock and Unlock of Cargo Door Lock
- Panic Button in Dash
- Panic Button Wireless/remote
    - Remote Vehicle Disabling
    - Remote Emergency Notification
- Electronic Cargo Seals
- Untethered Trailer Tracking
- Routing and Geofenced Mapping Software

A.4.2 Technologies by Truck

Tables A-8 and A-9 present the specific technologies that were installed on each of the 25 trucks that will be tested in this scenario. The suite of technologies are mapped to the technology tier described earlier as well as the functional requirements that were addressed.

A.4.3 Operational Description of Scenario

R&R and Dyno Transportation had used the satellite system extensively before and during the actual FOT. They both use the system for positioning, daily messaging, and operations. R&R also had the new capability to geofence some of their standard routes, which was also evaluated.

Driver identification was performed with the Biometric Login feature for all participants in this scenario. The drivers had to login using their fingerprint and smartcard after each time the tractor was started or had been disabled.

All three carriers had wired and wireless panic buttons installed in their tractors. The panic buttons were only used during on site evaluations with the evaluators. The Wireless Vehicle Disable (WVD) was also used during these controlled tests with the evaluators in a controlled environment to disable the throttle of the tractor.

All trucks in this scenario also had the ability to do electronic manifest. Orica utilized it with R&R shipping product to Scenica in Illinois. Dyno utilized it with R&R on runs to Orica in Indiana.

R&R had onboard computers (OBC) installed on their tractors. The functionality of these OBC's for loss of signal disabling and OTA disabling were tested on site at R&R in a controlled environment during the evaluation testing. The OBC also controlled the remote door unlocking device was used on daily runs from Charlestown to Joplin.

Table A-8. Technologies per Truck on Scenario 4a

Truck	Technologies							Tier	Shipper	Carrier	Functional Requirements
76	Satellite	Panic Dash/WPB/WVD	Bio Auth.	E-Manifest	OBC			T-5	Orica	R&R Truck	1.1-1.4,2.1-2.4,2.6,2.8,2.10-2.14,3.2-3.4
77	Satellite	Panic Dash/WPB/WVD	Bio Auth.	E-Manifest	OBC			T-5	Orica	R&R Truck	
78	Satellite	Panic Dash/WPB/WVD	Bio Auth.	E-Manifest	OBC			T-5	Orica	R&R Truck	
79	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	1.1-1.5,2.1-2.4,2.6, 2.10-2.12,2.14,3.2-3.4
80	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	
81	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	
82	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	
83	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	
84	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	
85	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	
86	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	
87	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest		Elec.Seal		T-6	Orica	R&R Truck	
							Geo-Map			R&R Truck	

Table A-9. Technologies per Truck on Scenario 4b

Truck	Technologies					Tier	Shipper	Carrier	Functional Requirements
88	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	1.1-1.5,2.1-2.3,2.5,,2.10-2.12,2.14,3.2-3.4
89	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
90	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
91	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
92	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
93	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
94	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
95	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
96	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
97	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	Unteth Trailer Tr.	T-5	Dyno	Dyno Trans	
98	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	WVD	T-4	Dyno	Dyno Trans	1.1-1.5,2.1-2.3,,2.10-2.12,2.14,3.2-3.4
99	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	WVD	T-4	Dyno	Dyno Trans	
100	Satellite	Panic Dash/WPB	Bio Auth.	E-Manifest	WVD	T-4	Dyno	Dyno Trans	

Lastly, Dyno Transportation had 10 trailers with tethered and untethered trailer tracking units. These trailers were of varying manufacturers and were spread out through their footprint of delivery locations.

Appendix B.
Hazmat Industry Technology Analysis

Introduction

The Hazardous Materials Security and Technology Analysis Tool provides an in-depth look at the hazardous materials industry as well as the technology deployment. The Analysis Tool contains specific information on company demographics, routing, hazmat hauled, security concerns and issues, and current and future use of security technologies. It contains unique information on technologies specifically geared towards the hazmat industry.

B.1 Objective

The Hazardous Materials Security and Technology Analysis Tool was produced to relate FOT findings with larger hazardous materials industry data. ATRI led this component of the FOT and contacted a number of the key members of the hazmat transportation industry. The data collection approach was developed with significant input from the Battelle Team, FMCSA, and the Independent Evaluation Team. Data for a small group of representative hazmat carriers were gathered to test the effectiveness of the proposed approach. Based on the results of that effort, revisions were made and the larger effort was undertaken. Ultimately, data on 164 hazmat carriers were obtained. These carriers were culled from several different carrier information databases such as the National Fleet Directory, intrastate databases, and the National Tank Truck Carriers membership.

B.2 Profile of Included Companies and their Fleets

Data from 164 trucking companies were obtained. Based on the information collected, ATRI believes the hazmat security topic is considered a "sensitive" issue to the hazmat industry, particularly given the government sponsorship of the survey and the concern over "increased regulations."

B.2.1 Fleet Size

The analysis tool collected data on the number of power units operated by their company. These were categorized using FMCSA-designated categories listed in Table B-1.

Table B-1. Number of Power Units Operated by Company Size

Category	Number of Trucks Operated	Percentage
Very Small	6 or less	8.5
Small	7 to 20	18.8
Medium	21 to 100	38.8
Large	100 or more	29.7
Unknown		4.2

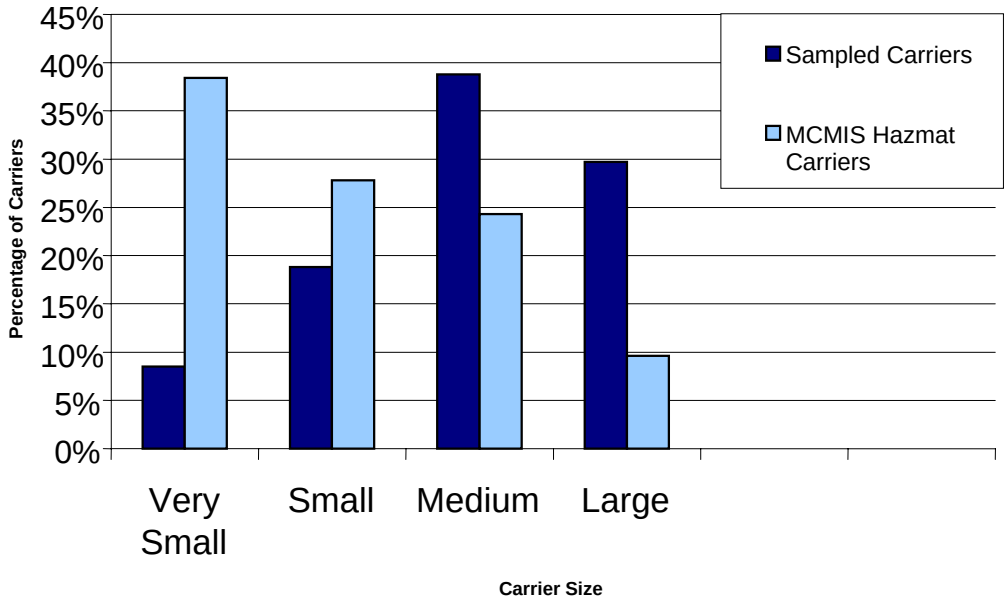

Figure B-1. Analysis of MCMIS Hazmat Carriers

Figure B-1 compares carrier size of those sampled in the hazmat industry technology analysis with active hazmat carriers within the Motor Carrier Management Information System – Census file (MCMIS).

The sampled carriers appear to show an inverse relationship to those listed in the MCMIS database. The American Trucking Associations' North American Fleet Directory database also indicates that the majority of HM "fleets" are composed of fewer than six trucks. The research team believes that three major rationalizations may explain the differences:

- Driver/Carrier Access Issues – Small carriers, often described as independent operators, are difficult to access for research purposes since they typically drive more than 100,000 miles every year.

- Carrier Security Concerns – Several Federal government studies have shown that smaller carriers have considerably greater security concerns and perceived vulnerabilities, along with fewer resources to address the issues. A recent USDA study[12] involving food transportation carriers found that larger carriers are more comfortable with their security programs and expend greater resources to manage security. The impact on the HM survey may be that larger carriers are better prepared (and staffed) to respond to research inquiries on security efforts and technology utilization.

[12] Development of a Guidebook for Identifying Security Management Practices in Agricultural and Food Commodity Transportation – Technical Memo #5 Survey Analysis, pg. 5, 2004.

- Carrier Fleet Size Versus HM Tonnage – The survey analysis didn't attempt to contrast fleet size by tonnage moved. However, American Trucking Associations' Freight Forecast to 2014 shows that large carriers are responsible for moving the majority of freight by tonnage. Interpolating this to the HM survey indicates that the large number of medium to large carrier survey respondents likely carry a substantial portion of all HM shipments.

B.2.2 Range of Operation

The range of operation and type of hazmat hauled for each carrier were determined. The average length of haul was stratified using categories from the 1997 Vehicle Inventory and Use Survey (VIUS) produced by the U.S. Census Bureau [1]. Table B-2 represents these categories:

Table B-2. Range of Operation Comparison

Category	Number of Miles	Percentage		
		FOT Industry Analysis	VIUS Hazmat Carriers	CVO Industry*
Local	Less than 50	15.8	30.7	39.5
Short range	51 to 100	18.2	19.0	16.7
Short range medium	101 to 200	21.2	10.9	10.8
Long range medium	201 to 500	28.5	17.4	12.2
Long range	More than 501	8.5	19.5	16.0
Unknown		7.9		

*These numbers derived from an August 2003 FMCSA database query.

For comparison purposes the percentages are compared with other data on the hazmat and general CVO industries. As can be seen, it was easier to obtain data for the longer-range carriers.

According to the American Trucking Trends 2003, 81.3 percent of trucking companies operate six or fewer trucks. This figure is substantiated by an FMCSA query performed in August of 2003 which shows 87.4 percent of carriers operating six or fewer trucks. Alternatively, companies included in the analysis comprise only 8.5 percent of this category. Since there is a large percentage of small (hazmat and non-hazmat) carriers, this difference between included companies and general industry weightings is possibly due to:

- The preponderance of larger carriers in the hazmat sector, and/or
- A greater comfort level by large carriers with providing hazmat information and data to the Deployment Team.

- It is well understood that the majority of the 585,000 for-hire U.S. interstate motor carriers[13] are individual owner-operators, controlling six or fewer trucks.

Emerging Points

- The largest respondent group (38.8 percent) was the mid-sized company which operates between 21 and 100 power units. This differs considerably from the general industry population of mid-sized carriers (hazmat and non-hazmat) at 3.4 percent.

- It is difficult to ascertain whether the differences in included company's fleet-size weightings reflects differences in hazmat versus general industry composition, or reporting issues.

- Given the volatility of fleet size reporting (e.g., 42 percent of the VIUS carriers reported operating less than six power units), documenting the statistical relationship of fleet size to hazmat transport may not be possible.

- Included companies' range of operation percentages most closely match the general industry in the "short-range" carriers grouping.

- The majority of included companies (28.5 percent) are categorized as long-range medium haulers.

For a variety of technical and security reasons, a carrier's range of operation may play a role in determining the applicability of security issues and strategies. Included company's average length of haul was categorized using breakouts from the 1997 Economic Census: Vehicle Inventory and Use Survey (VIUS) produced by the U.S. Census Bureau. The following represents responses from each of the breakout categories.

B.2.3 Route Variability

Hazardous materials carriers must adhere to strict routing. Hazmat routing is often dictated by both state and federal jurisdictions, but is usually managed at the state level. Based on current Federal regulations (49 CFR Part 397), there are several criteria used to determine hazardous materials routing such as population density, types and quantities of hazardous materials being shipped, terrain considerations, delays in transportation, congestion and accident history, etc.

A straight presentation of responses by carriers that transport hazmat as to the level of route variability (versus fixed or dedicated routes), does not allow for much analysis:

[13] American Trucking Trends 2003, American Trucking Association, 2003, p 6.

Level of routing variability

- 30 percent – Very variable
- 47 percent – Somewhat variable
- 21 percent – Not much
- 3 percent – Did not answer this question

When this information is considered in context with the number of respondents that listed "radioactive materials transportation" (4.9 percent) it becomes apparent that typical radioactive shipments are moved in relatively small quantities as compared to Class 3 Flammable Liquids.

The following compares responses on route variability (versus fixed routes) with ranges of operation (Table B-3)

- 77 percent of local operators reported having "very much to somewhat" route variability
- 80 percent of short-range operators reported having "somewhat to very little" route variability
- 54 percent of short-range medium operators reported having "somewhat" route variability
- 83 percent of long-range medium operators reporting having "very much or somewhat" route variability
- 64 percent of long-range operators reporting having "very much" route variability.

Table B-3. Comparing Route Variability with Range of Operation

Range of Operation / Route Variability	Local	Short-Range	Short-Range Medium	Long-Range Medium	Long-Range
Very Much	27%	17%	17%	36%	64%
Somewhat	50%	47%	54%	47%	21%
Very Little	12%	33%	29%	15%	14%
Not at all	12%	0%	0%	2%	0%

Emerging Points

- 77 percent of local operators reported having "very much to somewhat" route variability
- 80 percent of short-range operators reported having "somewhat to very little" route variability
- 54 percent of short-range medium operators reported having somewhat route variability

- 83 percent of long-range medium operators reported having very much or somewhat route variability
- 64 percent long-range operators reported having very much route variability.

B.2.4 Fleet Size in Comparison to Ranges of Operation

Given the unique characteristics associated with carrier size and range-of-operation, cross-factoring the two data sets may offer insight into the security vulnerabilities and opportunities associated with certain groupings. For example, small hazmat carriers with local routing may be considerably more difficult to manage during a high national threat level given their lack of technology utilization and technology limitations (e.g., line-of-sight issues with satellite).

Comparing motor carrier size to their average length of haul produces the following analysis as seen in Table B-4.

Table B-4. Comparing Motor Carrier Size to Average Length of Haul

Carrier Size	Local	Short-Range	Short-Range Medium	Long-Range Medium	Long-Range
Very Small	36%	29%	18%	7%	0%
Small	16%	42%	26%	6%	10%
Medium	16%	16%	20%	34%	9%
Large	12%	6%	20%	45%	10%

*Percentages may not total 100 due to rounding and/or multiple entries.

Emerging Points

- The majority of "large" motor carriers (55 percent) indicated moving hazardous materials in the long-range medium or greater category. However, a second-level cross-factoring with fleet characteristics (of large carriers who operate locally), indicates that 3.7 percent of these large local carriers are LTL carriers operating 150+ power units. This is consistent with the trucking industry's larger LTL, or pickup and delivery, trucking companies as previously noted.
- A large percentage of medium-sized carriers (34 percent) indicated their average length of haul as long-range medium.
- The majority of small carriers (42 percent) indicated their average length of haul as short-range.
- More than a third of very small carriers' respondents (36 percent) indicated their average length of haul as local.
- A strong positive correlation appears to exist between carrier size and length of haul.

B.2.5 Hazardous Materials Hauled

As expected, hazmat transporters move a wide variety of hazmat commodities. Figure B-2 presents a distribution of hazmat transported from the 1997 Commodity Flow Survey (U.S. Department of Transportation, Bureau of Transportation Statistics) for comparison purposes. Figure B-3 presents this distribution of HM transported based on analysis of FOT carriers.

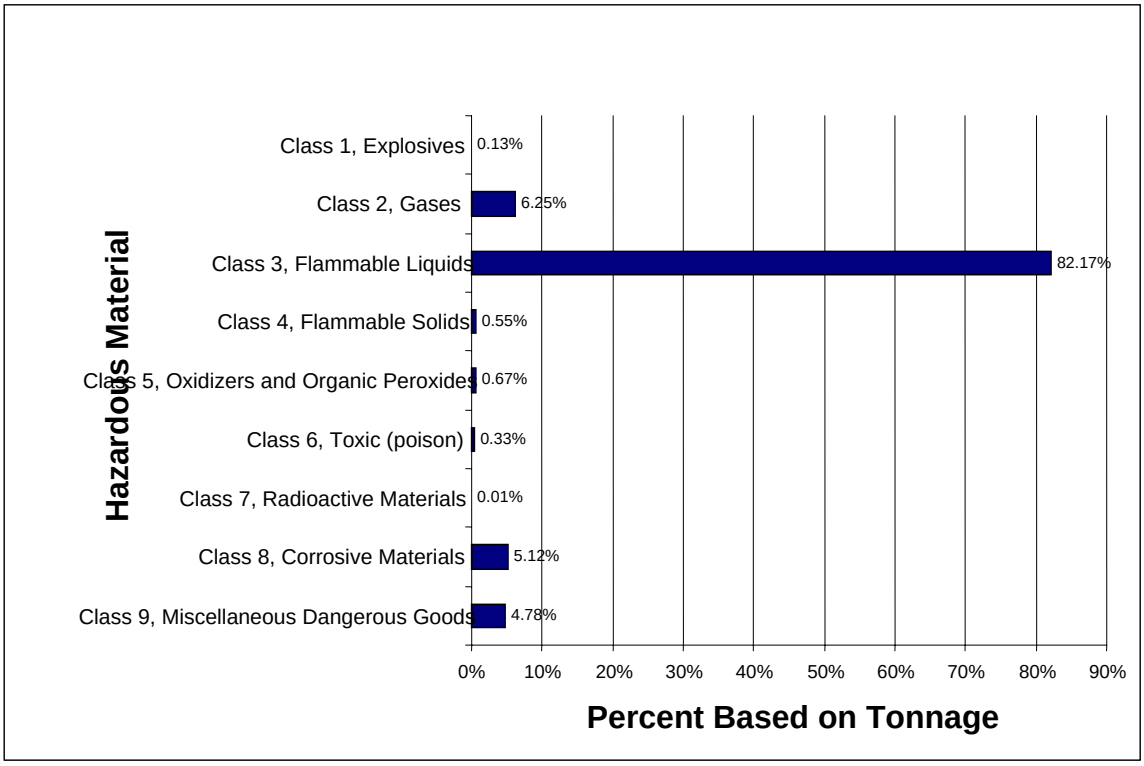

Figure B-2. Commodity Flow Survey 1997 – Hazmat Transported

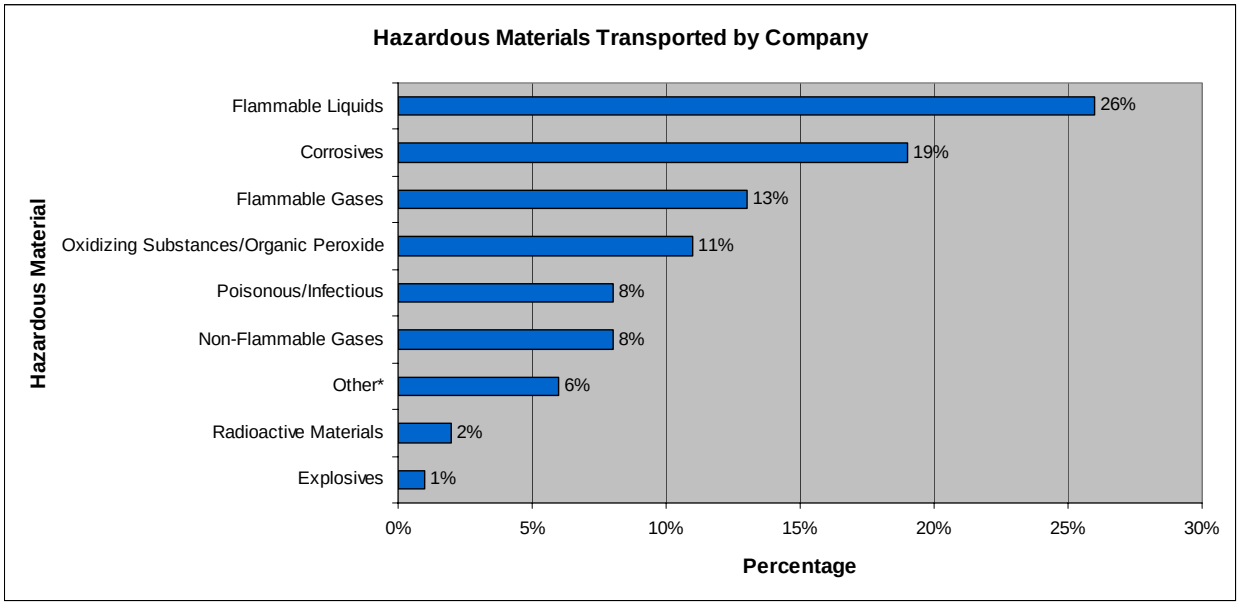

Figure B-3. FOT Industry Analysis of Hazardous Material Transported

Comparing the classifications of hazardous materials hauled by operation type, LTL or truckload, results in the following (Table B-5):

Table B-5. Comparing Classifications of Hazmat Hauled by Operation Type

Type of Hazardous Materials	Truckload	Less than Truckload
Explosives	2%	10%
Flammable Gases	36%	35%
Non-Flammable Gases	23%	25%
Flammable liquid	69%	75%
Poisonous/Toxic Gases	17%	10%
Flammable Solid	16%	35%
Oxidizing Substances	29%	30%
Poisonous/Infectious	20%	15%
Radioactive material	4%	10%
Corrosives	53%	45%
Other	17%	20%

*Percentages may not total 100 due to rounding and/or multiple entries.

Emerging Points

- Approximately 88 percent of the included companies indicated their company type as Truckload.

- Ten percent of included LTL companies reported hauling explosives, while truckload respondents reported only two percent. This difference was again present in radioactive materials and flammable solids. Ten percent of included LTL companies reported hauling explosives, while truckload respondents reported only two percent. This difference was again present in radioactive materials and flammable solids. Based on data from the included companies, it would appear that LTL operators are more likely to haul explosives, radioactive materials and flammable solids than truckload respondents.

- According to the *Commodity Flow Survey, Hazardous Materials* (FHWA, 1999, Table 2), 80.8 percent of total tonnage of hazardous materials were Class 3 Flammable Liquids, transported an average of 73 miles per shipment.

When company size is cross-tabulated with the hazmat classification transported, the following distributions occur as shown in Table B-6.

Table B-6. Cross Tabulation of Company Size and Hazmat Transported

Hazmat Classification	Very Small	Small	Medium	Large
Explosives	0%	0%	3%	6%
Flammable Gases	0%	26%	22%	56%
Non-Flammable Gases	7%	0%	17%	44%
Flammable liquid	64%	61%	66%	56%
Poisonous/Toxic Gases	0%	0%	13%	39%
Flammable Solid	7%	10%	19%	28%
Oxidizing Substances	7%	10%	30%	28%
Poisonous/Infectious	0%	0%	19%	28%
Radioactive material	8%	0%	5%	17%
Corrosives	21%	23%	53%	56%
Other	14%	13%	11%	22%

Emerging Points

- Flammable liquids appear to be hauled by all fleet sizes.
- Medium and large companies haul more poisonous and infectious materials based on the data.
- Large motor carriers were almost four times more likely to carry radioactive material than the other three categories on average.

- No carriers with less than 20 power units reported to transporting explosives or poisonous/infectious materials.

B.3 Leading Security Concerns and Issues

The number and variety of security concerns and issues have multiplied for trucking companies since the tragic events of September 11, 2001. With new security legislation, trucking companies are faced with myriad issues that must be accounted for to ensure safe, compliant transport of commodities. The analysis tool identified the leading security concerns and/or issues relating to hazardous materials transport for the included companies. The Figure B-4 documents the majority of security concerns/issues with the corresponding numbers of those rated in the top five.

B.3.1 Security Concerns and Issues

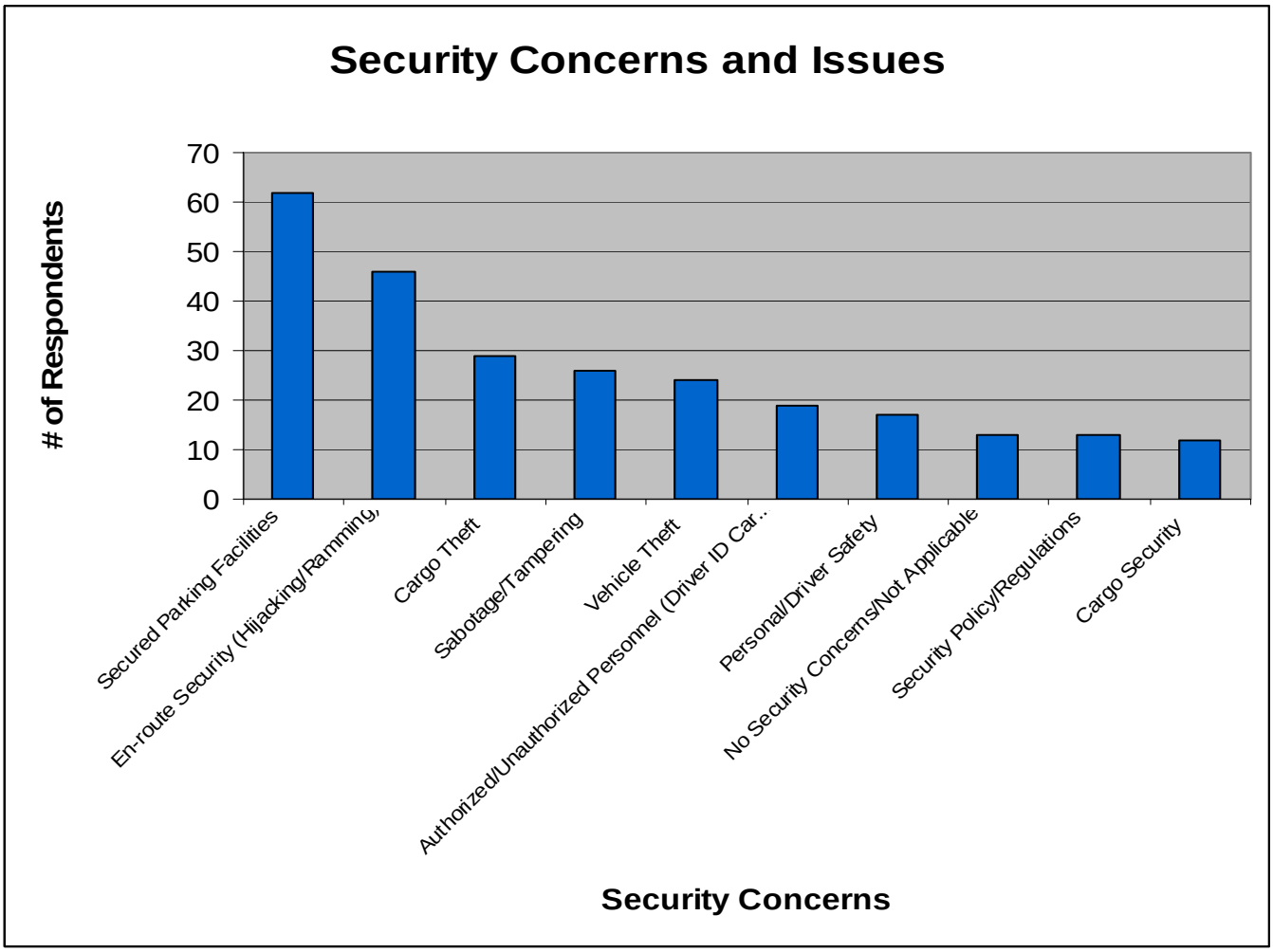

Figure B-4. Analysis of Security Concerns and Issues

Prior to September 11, 2001, cargo theft was the primary security issue based on anecdotal industry information, and continues to be a critical issue. Included companies also listed vehicle theft as one of their top security concerns; when "vehicle security" is included with "vehicle theft", the category moves into the top three issues. "Secured parking facilities" was not listed specifically as an issue but was often cited as a solution to vehicle theft/security as well as "en-route security." Secure parking facilities, both at the terminal, and while on the road are extremely important to security. Cargo security, traffic congestion, and awareness of security concerns were among some of the others listed. It is quite clear that the trucking industry and hazmat transporters in particular, have a large number of legitimate security concerns.

Nevertheless, it was surprising that a significant number of carriers indicated that they have no hazmat security concerns. Despite the media attention highlighting possible HM terrorist activities, more than 10 percent reported that they didn't have any security concerns.

When security concerns were compared with the range of operation, the following distributions arose as seen in Table B-7.

Table B-7. Comparing Security Concerns with Range of Operation

Range of Operation	Local	Short-Range	Short-Range Medium	Long-Range Medium	Long-Range
Concern #1	En-Route Security	Cargo Theft	En-Route Security	Cargo Theft	Cargo Theft
Concern #2	Terrorism/ Access by Terrorists	Secured Parking Facilities	Cargo Theft	Secured Parking Facilities	Secured Parking Facilities
Concern #3	Cargo Theft	Terrorism/ Access by Terrorists	Secured Parking Facilities	Cargo Security	En-Route Security

This comparison illustrates that despite a trucking company's range of operation, their top concerns are universal. The three most common concerns are:

1. En-route security
2. Cargo theft
3. Sabotage and tampering

B.4 Technologies, Programs, and Policies Most Likely to Improve Security

Information, support, and training strategies that a carrier would want available to address its security concerns and/or issues were collected using the analysis tool. Figure B-5 depicts carrier responses and suggestions.

B.4.1 Carrier-Requested Support

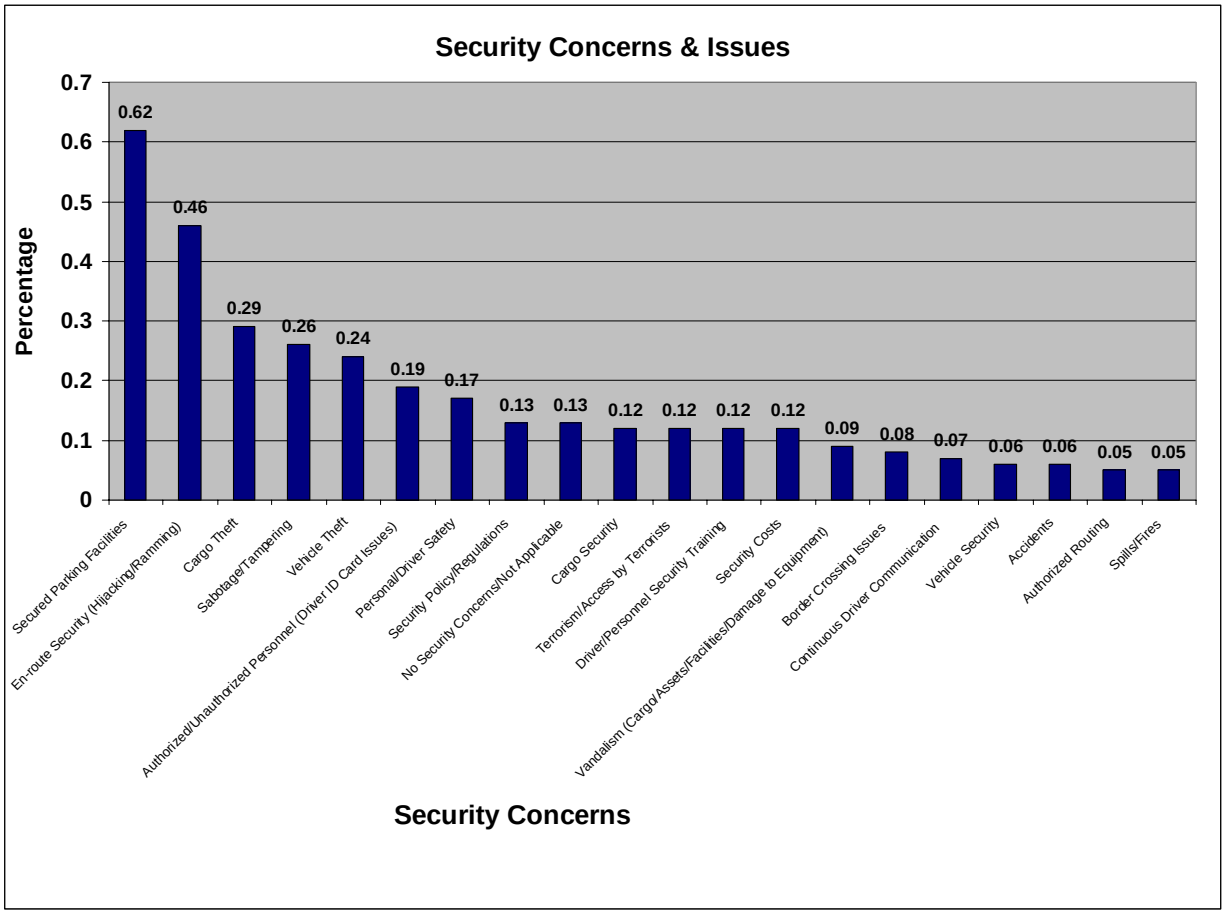

Figure B-5. Company Security Concerns and Issues

Figure B-5 illustrates the general suggestions proffered by the hazmat respondents for addressing security concerns and issues. Updates on security technologies, standardized technologies, updates on security legislation, and security alert bulletins were stated as strong possibilities for supporting the hazmat trucking industry. Also mentioned were alternative funding such as government investment subsidies, and the need for a security best practices guidebook.

B.5 Recommended Technologies and Procedural Solutions

The solutions that included companies use currently, or will incorporate in the future, to address their security issues were identified. As expected, there were a variety of solutions. Table B-8 lists the prominent solutions and technologies as well as the number of included companies that have or will adopt them.

B.5.1 Security Solutions

Table B-8. Security Solutions

Suggested Solution	No. of Respondents
Simple Antitheft Devices & Measures	57
Vehicle Satellite Tracking	35
Secure Parking/Facilities	24
Company Security Plan	19
Communication Devices	18
Driver ID's	16
Cell Phones	13
Customer/Driver Background Checks	9
Driver Call-In/Check-In	8
Change in Routing	7
Pre & Post Trip Inspections	7
Driver Awareness	3
Hazardous Materials Highway Watch Program Qualified Drivers	3
No Preloading	3
Driver Hiring Practices	3
Change in Delivery Times	2
Customer Training	2
Trailer Tracking Systems	1
Customer Route & Schedule Review	1
Driver Authorization System	1
Proper Placards	1

Emerging Points

- Simple antitheft devices and measures, such as keeping tractor and trailer locked at all times, were the most common carrier solutions.
- Use of vehicle satellite tracking was the second most common security solution or technology identified.

B.6 Technologies Currently Used by Carriers and Future Considerations

A key objective of the analysis tool was to determine which technologies are in use today, and which technologies carriers are likely to purchase for their fleets in the future. For the purposes of this analysis, "future" was defined as the next two to three years. The analysis tool also

gathered a listing of vendors for each technology used. Figure B-6 captures the current and future use of these technologies.

B.6.1 Current and Future Technologies

Figure B-6 is a comparison of technologies that are currently used and their potential future use.

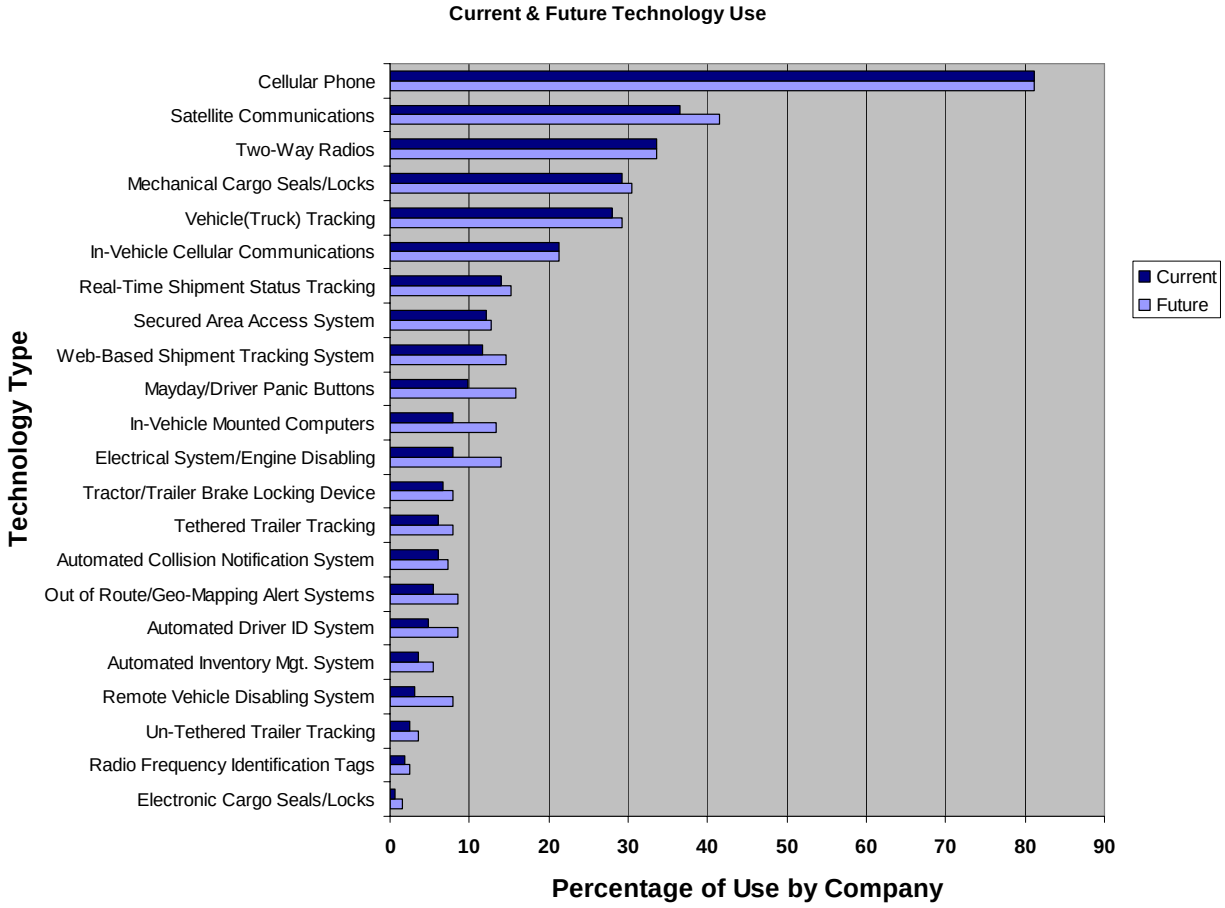

Figure B-6. Company Current and Future Technology Use

As illustrated above, the trucking industry has and will in the future embrace a range of security technologies. Current technologies most frequently used by the represented companies are cell phones, vehicle tracking, and satellite communications. As well, these are among some of the most mature technologies on the market.

Emerging Points

- Vehicle (truck) tracking continues to expand within the mainstream trucking industry.
- Wireless communications appear to be used by a considerable number of respondents, and will continue to expand in the future based on the data collected.

B.7 Summary Analysis

The analysis, comprised of data from 164 companies, targeted four key areas of interest: (1) profile of respondents and their fleets; (2) leading security concerns and issues; (3) technologies, programs and policies most likely to improve security; and (4) recommended technologies and procedural solutions.

B.7.1 Profile of Included Companies and their Fleets

The majority of included hazmat companies (82 percent) operate between 7 and 100 power units. This appears to be a somewhat inverse relationship to the American Trucking Trends 2003, which states that 81.3 percent of trucking companies operate six or fewer trucks[14]. Since the full database of included companies contains a large percentage of small (hazmat and non-hazmat) carriers, this percentage difference between companies included and general industry weightings is possibly due, as previously stated, to: the preponderance of larger carriers in the hazmat sector; greater comfort level by large carriers with providing hazmat information and data to the Deployment Team; and/or the definition and impact of owner-operators on the total carrier populations. Table B-9 compares respondent size to the industry by operating range.

Table B-9. Comparison of Respondent Size to the Industry, by Operating Range

Category	Number of Miles	FOT Industry Analysis (percentage)
Local	Less than 50	15.8
Short range	51 to 100	18.2
Short-range medium	101 to 200	21.2
Long-range medium	201 to 500	28.5
Long range	More than 501	8.5
Unknown		7.9

[14]American Trucking Trends 2003, American Trucking Associations, 2003 p.v.

Hazmat transporters move a wide variety of hazmat commodities. The type of hazmat hauled as well as other variables were determined by the analysis. Ten percent of LTL respondents reported hauling explosives, while truckload respondents reported only two percent. This difference was again present in radioactive materials and flammable solids. Based on the data collected, it would appear that LTL are more likely to haul explosives, radioactive materials and flammable solids than their counterparts, truckload respondents. According to the *Commodity Flow Survey, Hazardous Materials* (FHWA, 1999, Table 2), 80.8 percent of total tonnage of hazardous materials were Class 3 Flammable Liquids, transported an average of 73 miles per shipment.

B.7.2 Leading Security Concerns and Issues

The analysis tool asked respondents to list their five leading security concerns and/or issues relating to hazardous materials transport. The top three ranked issues were en-route security, cargo theft, and sabotage and tampering. Prior to 9/11, cargo theft was the number one issue based on previous surveys, and continues to be a critical issue. Respondents also listed vehicle theft as one of their top security concerns; when "vehicle security" is included with "vehicle theft", the category moves into the top three issues. When security concerns were compared with the range of operation, the following distributions arose: en-route security; cargo theft; and sabotage and tampering.

B.7.3 Technologies, Programs, and Policies Most Likely to Improve Security

The analysis tool solicited information, support, and training strategies that a carrier would want available to address its security concerns and/or issues. Updates on security technologies, standardized technologies, updates on security legislation, and security alert bulletins were stated as strong possibilities for supporting the trucking industry. Also mentioned were alternative funding such as government subsidies and security best practices.

B.7.4 Recommended Technologies and Procedural Solutions

Respondents were asked to list any solutions that they use currently, or will incorporate in the future, to address their security issues. As expected, there were a variety of responses. Simple antitheft devices and measures such as keeping the tractor and trailer locked at all times were the most common carrier responses. Use of vehicle satellite tracking was the second most common carrier response.

The analysis tool also determined which technologies are in use today, and which technologies carriers are likely to purchase for their fleets in the future. Current technologies most frequently used by respondents are cell phones, vehicle tracking, and satellite communications. These are among some of the most mature technologies on the market. Vehicle (truck tracking) continues to move into the mainstream trucking industry. Satellite communications appear to be used by a number of companies and appear that they will continue to be in the future.

Appendix C.
Technology Compendium

The companies and/or products or services listed in this publication are included because they have been described by the vendor as offering similar functionality to the technologies tested as part of the Hazmat Safety and Security Field Operational Test. The authors and sponsors have not independently verified the accuracy of the vendor's descriptions and thus make no representations as to the functional similarity. Inclusion of specific company products or services in this Compendium is not, and should not be construed as, an endorsement by the authors (or sponsors) of those products or services.

Introduction

The Technology Compendium is a compilation of trucking industry technologies currently in the marketplace. In addition, vendors that were unable to participate were also interested in submitting product information. Information on each of the security technologies and companies was submitted voluntarily or identified through secondary research and compiled. This information includes contact data, product functionality, market penetration and pricing. Many of these technologies are similar in functionality to those tested in the FOT.

C.1 Methodology

As a major component of the FOT, the Technology Compendium began as a way to recognize the myriad technologies and systems on the market. Efforts to include these vendors and their technologies began with an area for input on the safehazmat.com website in which interested companies could enter in their product information for inclusion in the compendium. In addition, internet searches were performed. Companies were contacted via phone and e-mail, and approximately 35-40 interviews were performed to garner more detailed product information. For those companies that did not respond to telephone messages, faxes and initial e-mails, an e-mail was sent out with their segment of the compendium spreadsheet.

Several presentations on the FOT at various events and conferences have led many other vendors to the safehazmat.com website. Interviews were also conducted at the 2003 American Trucking Associations Management Conference and Exhibition in San Antonio, Texas. Articles in several industry publications, such as Transport Topics, have also publicized the Technology Compendium.

C.2 Purpose

The FOT tested a number of technologies in several different areas such as vehicle communications, cargo seals, vehicle disablement, etc. The relative small size of the test, 100 vehicles, and the large number of technologies being tested made it impossible to include other vendors in the actual FOT. It was determined that a compendium of current security technologies, similar to those tested in the FOT, would serve several purposes. The first would be a place for interested vendors to include their products in a prominent national FOT. Furthermore, the FOT does not endorse any one product, and a comprehensive listing of myriad technologies provides an accurate picture of other security technologies in the marketplace.

C.3 Results

The Technology Compendium currently consists of a Microsoft Excel spreadsheet. The spreadsheet compiles contact information, product functionality and description, current market penetration, and pricing information for 94 different companies. These 94 different companies represent 147 technologies. Of the 147 different technologies represented, approximately 52 companies, or 35 percent, shared some type of pricing schemes. The following is a breakout and description for each category.

C.3.1 Anti-hijacking/Security

This category is represented by 2 products from 2 different companies. They are listed below.

1. Vericom
2. Zonar

Each of these products is uniquely different. Vericom's product, Veriguard, is a covert system that ensures driver authentication and performs vehicle disablement when an unauthorized driver attempts to take a vehicle. Zonar's EVIR is a series of RFID tags placed at strategic points on a truck or bus in accordance with a pre-trip inspection. These RFID tags are read by a handheld reader when a driver comes into close proximity with them, ensuring that a driver performs a pre-trip inspection correctly.

Pricing: There is currently no pricing information available on these products.

C.3.2 Asset Securement

This category is represented by only one company as listed below.

1. Engineered Inerting Systems

This Explosion Suppressant Arresting Foam protects tanker trucks carrying flammable and explosive materials. This is a unique product that has the ability to suppress an explosion and minimize the effects.

Pricing: There is currently no pricing information available for this product.

C.3.3 Asset Tracking

Asset tracking systems consist of many different satellite and terrestrial units primarily used to track trailers and large construction equipment. These systems use different technical approaches to "track" vehicles ranging from satellite and terrestrial triangulation to GPS-based locators. In some instances, fixed site readers are used; although these are presently quite limited, new indicators are that major shippers will begin to increase their use of Bluetooth and RFID readers. There are 21 products representing 16 different companies which are as follows:

1. Aether Systems, Inc.
2. Aircept
3. Datacom
4. Fleetilla
5. General Electric
6. GPS Management
7. Intermodal Security Devices
8. Lat-Lon, LLC
9. Mobilearia, Inc.
10. PAR Technologies
11. Qualcomm
12. SkyBitz
13. TeleTouch
14. Terion
15. TrackStar
16. V-TRAC Systems, INC

Pricing: Basic tracking units retail for $139 to $500. Mid-range price of these units were approximately $375 to $450. The majority of the companies offer discounts based on larger quantities. Tracking units primarily used for tracking large construction equipment, were priced anywhere from $500 to $2000. These more expensive devices often were elevated in price because of their ability to integrate different types of sensors.

Installations for the basic tracking units range between $30 and $125. A couple of the companies offered installation included in the base price of the unit. The more rugged construction oriented units have higher installation costs because of different sensor options. Their installation costs range between $500 and $2000.

Monthly fees differed based on different communication patterns, i.e., the number of times the unit reports its location. These monthly service fees ranged from $4.99 to $15. These costs can fluctuate greatly dependent on the customer preference on number of location reports.

C.3.4 Biometrics

Biometrics consists of a variety of biometric authentication devices ranging from fingerprint to facial recognition. Some of these products already have or are able to integrate the use of smartcards. There are 17 products representing 17 different companies which are as follows:

1. AcSys Biometrics Corporation
2. ActivCard
3. AuthenTec
4. Biocentric Solutions Inc.
5. Bioidentix
6. Bio-Key International
7. Cogent Systems
8. Compu-Trol Technologies Inc.
9. Cross Match Technologies, Inc.
10. Cyber Sign Inc.
11. Data Management Inc.
12. Digital Persona, Inc.
13. exResource
14. FingerSec
15. Hectrix
16. Identix
17. Saflink Corporation

Pricing: For pricing information available, the biometric products range from $6 to $1200. The $6 biometric component is the actual fingerprint sensors and this specific company partners with manufacturers and vendors to provide biometrics to OEM and ODMs. The more expensive units utilize better fingerprint reading technology and are complete systems. Average pricing is approximately $1000, and most of the systems have the ability to integrate with smartcards and other technologies.

These biometric products listed no installation of monthly service fee.

C.3.5 Cargo Seals

The cargo seal category ranges from low-end tapes and seals to GPS enabled e-seals. There are 6 products represented by 3 companies listed below:

1. Bulldog Technologies
2. CGM Security Systems
3. Savi Technologies

Pricing: The basic self-adhesive seals and metal clips range from $545 for a carton to $1.59 per seal with discounts on quantities. The seals utilizing GPS and/or wireless technology range from $1,195 to $1,495 per unit. These prices are per unit, and many of those listed do not require software as they are accessed through the internet.

Installation can be done by the customer, so there are no associated fees.

No information on monthly service fees is currently available.

C.3.6 Employee Emergency

There is one product represented in this category. This product provides employees with a distress signal if they are hurt or incapacitated.

1. TeleTouch

Pricing: There is currently no pricing information available for this product.

C.3.7 Locks

This category contains basic locking mechanisms such as Kingpin locks as well as wireless internal door locks. There are 12 different products represented by 7 different companies that are listed below:

1. Cargo Protectors, Inc.
2. CGM Security Systems
3. Porter Technologies
4. Power In-Lock
5. Tomal Systems, LLC
6. Transport Security, Inc-ENFORCER®
7. Wapner Truck Alarm Systems, Inc.

Pricing: Some basic locking devices for air brakes range from $195 to $333 per unit with discounts on quantities. The more technologically advanced locking devices are internal and require the driver to request access in order for the door to open. These types of devices range from $432 to $595 and can be integrated with a pager and/or other tracking systems. In terms of information provided, none of these locking devices require a software program as they are stand alone products. However, as mentioned before, some of the more technologically advanced locks could be integrated with some form of wireless communication.

Pricing information on installation of the internal locks was not available.

There is no monthly service fees associated with the locks.

C.3.8 Software

The software category contains integration software, supporting software for some technologies, and mapping and fleet management software. There are 26 software products representing 17 different companies which are as follows:

1. Agentek, INC
2. Air IQ, Inc.
3. ALK Technologies, INC
4. Integrated Decision Support Corporation
5. Maddocks
6. Magnasoft Spatial Services, Inc.
7. Maptuit Corp.
8. McLeod Software Corp.
9. Object FX Corporation
10. Qualcomm
11. Saflink Corporation
12. Telcontar
13. TeleTouch
14. Software Company
15. TMW Systems
16. TrackStar
17. UPS Logistics Technologies

Pricing: Due to the many different configurations and applications of the software programs, there was very little pricing information available. However, for those able to provide pricing information, software site licenses range from $10,000 to $33,000 which would be fleet wide licenses allowing more than one terminal to use the software. Some technology vendors sell their software that is associated with a product. One company that does this provided a $995 software price per power unit. The software programs represent several different categories. They are as follows:

- Software associated with a specific technology such as Qualcomm's TrailerTRACS program which supports the tracking.
- Software that supports vehicle tracking.
- Mapping software, such as Spatial FX, which provides mapping and routing capabilities and integration with vehicle tracking systems.
- Fleet management software which may include engine diagnostic and maintenance information, hours of service information, etc.

C.3.9 Vehicle Tracking

The vehicle tracking category contains tracking products utilizing satellite, terrestrial, or hybrid tracking technology. There are 61 different products representing 46 different companies as listed below:

1. Advanced Productivity Computing
2. Aeris.net
3. Aether Systems, Inc.
4. Air IQ, Inc.
5. AirLink, Inc
6. AtRoad
7. Avel-Tech
8. Burdilla Lanser Technologies LLC
9. Cabit Systems
10. Cheetah Software Systems
11. Cloudberry Wireless Services
12. CSI Wireless
13. EarthTRAK
14. Fleetilla
15. GE TIP
16. Global 2-Way
17. GPS Management
18. Ida Corporation
19. Insight USA
20. InterTrak
21. IRD, Inc
22. Lorantec Systems, Inc.
23. Metler Toledo
24. Minor Planet
25. Mobilearia, Inc.
26. Network Innovations
27. Northwest Nuclear, LLC
28. Orbcomm
29. Pana-Pacific
30. PeopleNet Communications Corporation
31. PowerLoc Technologies, Inc.
32. Qualcomm
33. Safefreight Technologies
34. Sage Quest
35. Satellite Security Systems of North America
36. Telemisphere LLC
37. TeleTouch
38. Telogis
39. TrackStar
40. Transcore
41. Trimble
42. Vericom Technologies
43. Vistar
44. V-TRAC Systems, INC
45. Waveburst Communications, Inc.
46. Xata

Pricing: Due to the competitive nature of the vehicle tracking market, some companies were unwilling to provide pricing information. However, a number of companies volunteered pricing. Per unit base costs range from $429 to $2,275. The less expensive tracking represents turnkey solutions and pricing ranges from $429 to $995 for some of these technologies. The more expensive tracking technologies are integrated units with many options and range in price from $1,290 to $2,275.

Installation costs vary from $75 to $300. Some of the technologies can be installed by the company if desired.

Monthly service fees vary greatly dependent on how the customer configures location status. These fees range from $10 to $50. The service fees can be dependent on the method of wireless used (i.e., satellite, terrestrial, or hybrid), which uses both satellite and terrestrial. Terrestrial monthly fees will cost less than satellite monthly fees.

					Demographic Information								
Company	**Contact**	**Title**	**Phone**	**Fax**	**Address**	**City**	**State**	**Zip**	**E-mail**	**Website**	**Technology Area**	**Product**	**Function/Description**
Vericom Technologies	John Bjorn	President	410-381-5707	410-381-7417	9881 Broken Land Pkwy, Suite 400	Columbia	MD	21046	jbjorn@vericomtech.com	www.vericomtechnologies.com	**Antihijacking/Security**	Veriguard	Veriguard is a stand-alone security system that disables a vehicle down to 1000 rpms when an unauthorized driver does not correctly tap out the code. Has the ability to use biometrics and nine live points for the driver authentication process. It also has the ability to integrate with GPS and other wireless capabilities.
Zonar	Brett Brinton	President/CEO	206-878-2459		19518 International Blvd.	Seattle	WA	98188	brett@zonarsystems.com	www.zonarsystems.com	Antihijacking/Security	EVIR System	EVIR is a system and process to ensure the performance of visual safety and security inspections. The system functions through use of a ruggedized handheld RFID reader and RFID tags placed strategically around a vehicle to ensure at a minimum that the operator was in close proximity to the items to be inspected. An inspection prompts a user to inspect certain areas of a vehicle and then saved and transmitted wirelessly to a web-based application. Any exception-based condition reports would be sent via e-mail alerts.
Engineered Inerting Systems	George Salamy	Vice President	201-995-1457 ext 120	201-995-9504	545 Island Way	Ramsey	NJ	7446	gfsalamy@engineeredinerting.com	www.engineeredinerting.com	**Asset Securement**	Explosion Supressant Arresting Foam	Protects tanker trucks carrying flammable and explosive materials.
Aether Systems, Inc.	Michael Brown	V.P., Product Marketing	972-301-2702	410-654-6554	11460 Cronridge Drive	Owings Mills	MD	21117	mbrown@aethersystems.com	www.aethersystems.com	**Asset Tracking**	TrailerMax	TrailerMax utilizes GPS satellite lcoation reporting, identify trailer status on a long-life battery.
Aether Systems, Inc.	Michael Brown	V.P., Product Marketing	972-301-2702	410-654-6554	11460 Cronridge Drive	Owings Mills	MD	21117	mbrown@aethersystems.com	www.aethersystems.com	Asset Tracking	GoeLogic	GeoLogic provides real-time trailer tracking with GPS satellite location. It allows for un-tethered operation as well as tracking, trailer lock down, on-demand location reporting and time and distant sensitive tracking.
Aircept			1.877.684.2040						indirectsales@aircept.com	www.aircept.com	Asset Tracking	eTrailerTrack	
Datacom			450-681-6667		440 Armand-Frappier Blvd, Suite 350	Laval, Quebec	Canada	H7V 4B4	services@datacom.com	www.datacom.com	Asset Tracking	Echo	
Fleetilla	Dennis Reno		(734) 362-3260		1650 West Jefferson	Trenton	MI	48183	info@fleetilla.com	www.fleetilla.com	Asset Tracking	FL 1700 Trailer Tracking	Uses satellite communications to track un-tethered trailers.
General Electric	Jennifer Weeks	GE Verwise Application Manager	(610) 648-6700		426 West Lancaster Ave.	Devon	PA	19333	jennifer.weeks@ge.com	www.geverwise.com	Asset Tracking	Vehicle Location/Tracking	Untether Trailer Tracking Solution
GPS Management									info@gpsmanagement.com	www.gpsmanagement.com	Asset Tracking	MB-3000 MLU	Mobile Location Unit tracks assets as well as maps, uses geo-fencing, vehicle disablement.
Intermodal Security Devices	Robert Miller	President	888 DROPLOC	562/598-2400	270 Bristol Street	Costa Mesa	CA	92626	rjrwm8@worldnet.att.net		Asset Tracking	DropLoc Barrier Seal	Prohibits entry and supports in process status monitoring
Lat-Lon, LLC	John Felty	National Sales Manager	877-300-6566	303-531-5754	4251 S. Natches Court, Unit C	Sheridan	CO	80110	john@lat-lon.com	www.lat-lon.com	Asset Tracking	RoadRider	Security / chemical detection / location
Lat-Lon, LLC	John Felty	National Sales Manager	877-300-6566	303-531-5754	4251 S. Natches Court, Unit C	Sheridan	CO	80110	john@lat-lon.com	www.lat-lon.com	Asset Tracking	RailRider	Location, multiple sensors
Mobilearia, Inc.	Karl Mehta	Vice President	650-237-4405	650-937-1078	800 West El Camino Real, Suite 240	Mountain View	CA	94040	info@mobilearia.com	www.mobilearia.com	Asset Tracking	ContainerSecure™	Secures containers through use of container mounted sensors and remote sensor readers to detect tampering.
PAR Technologies			315/738-0600		8383 Seneca Turnpike	New Hartford	NY	13413	marketing@parlms.com	www.parlms.com	Asset Tracking	Cargo Mate	Collects location, status, association, and time-stamped data via wireless providers from rugged, multi-dimensional sensors affixed to transport assets and cargo.
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.comm	www.qualcomm.com	Asset Tracking	TrailerTRACS	
SkyBitz	Roni Taylor	Marketing	703-478-2364	703-478-3301	45365 Vintage Park Plaza, Suite 210	Dulles	VA	20166	rtaylor@skybitz.com	www.skybitz.com	Asset Tracking	InSight Security	Using GLS, InSight Security allows you to gain location visibility of trailers as well as monitor door open/close and tether/untether. The web application utilizes mapping, address lookups, email alerts and paging single trailers for position reports.
SkyBitz	Roni Taylor	Marketing	703-478-2364	703-478-3301	45365 Vintage Park Plaza, Suite 210	Dulles	VA	20166	rtaylor@skybitz.com	www.skybitz.com	Asset Tracking	InSight Cargo	Using GLS, InSight Cargo monitors cargo and trailer location as well as allowing the user, through a web application, to map locations, locate assets, record dwell times, prioritize a panic operation, perform address lookups, and receive e-mail alerts.
SkyBitz	Roni Taylor	Marketing	703-478-2364	703-478-3301	45365 Vintage Park Plaza, Suite 210	Dulles	VA	20166	rtaylor@skybitz.com	www.skybitz.com	Asset Tracking	InSight Tracking	Using GLS, InSight Tracking provides trailer tracking information via satellite. It allows the user to map locations, page trailers for location, lookup addresses, receive e-mail alerts, and prioritize a panic.
TeleTouch	Archie Connor	General Manager of 2-way paging	903.535.7800		110 North College Avenue, Suite 200	Tyler	TX	75702	info@teletouch.net	www.teletouch.com	Asset Tracking	GeoTrax	to report location of detached trailers.
Terion	Chris Hines	VP, Sales	972-398-7300	972-398-7305	6505 Windcrest Dr, #200	Plano	TX	75024	chines@terion.com	www.terion.com	Asset Tracking	FleetView™ Trailer Management System	Provides real-time and sensor information to track trailers.
Terion	Chris Hines	VP, Sales	972-398-7300	972-398-7305	6505 Windcrest Dr, #200	Plano	TX	75024	chines@terion.com	www.terion.com	Asset Tracking	FleetView™ Trailer Cargo Sensor	Uses ultrasonic high-frequency to detect cargo and timestamps loading and unloading of cargo.
TrackStar	Terri Recknor	President	315-721-0931	315-721-0934	8382 Seneca Trunpike	New Hartford	NY	13413	terrir@trackstar.com	www.trackstar.com	Asset Tracking	Track Star® Loc8r	This battery or vehicle powered device tracks trailers and other things such as containers with GPS technology. It maps location for the user.
V-TRAC Systems, INC	Lee Moore	President	877-273-7434	877-273-7164	230 Colfax Avenue	Grass Valley	CA	95945	lee@vtracsystems.com	www.vtracsystems.com	Asset Tracking	V-Link	V-Link uses GPS technology to track trailers through satellite. It sends position report and can differentiate between moving trailers within a yard and over-the-road operations.
AcSys Biometrics Corporation			905-634-4477	905-634-1101	P.O. Box 1670	Orange Beach	AL	36561	info@acsysbiometrics.com	www.acsysbiometrics.com	**Biometrics**	AcSys FRS	face recognition
ActivCard			510.574.0100	510.574.0101	6623 Dumbarton Circle	Fremont	CA	94555	jwhite@activcard.com	www.activcard.com	Biometrics	ActivCard	smart card-based authentication and digital signature
AuthenTec			321.308.1300	321.308.1430	709 S. Harbor City Blvd., Suite 400	Melbourne	FL	32901		http://www.authentec.com/	Biometrics	FingerLoc- physical access product;EntrePad-optimized for integration into phone computers	semiconductor company who provides fingerprint sensors
Biocentric Solutions Inc.			608.821-0821	608.821.0822	8417 Excelsior Drive	Madison	WI	53717	sales@beyondLSI.com	http://www.biocentricsolutions.com	Biometrics	CombiFamily	fingerprint identification for cell phones, credit cards, doorknobs, PCs
Bioidentix			281-464-2300	832-201-0558	13850 Gulf Freeway, Suite 250	Houston	TX	77034	info@bioidentix.com	www.bioidentix.net	Biometrics	BioTools v3™	
Bio-Key International			651.687.0414	651.687.0515	1285 Corporate Center Drive, Suite 175	Eagan	MN	55121	information@bio-key.com	www.bio-key.com	Biometrics	WEB-key	fingerprint identification
Cogent Systems			626.799.8090	626.799.8996	209 Fair Oaks Ave.	Pasedena	CA	91030	info@cogentsystems.com	www.cogentsystems.com	Biometrics	Securearm, BioGate	fingerprint recognition hardware and software
Compu-Trol Technologies Inc.			516.679.2737	516.679.2734	2080 Wantagh Ave	Wantagh	NY	11793	bolinfo@compu-trol.com	www.compu-trol.com	Biometrics	Biometric Operator Log (not on the market yet); Sober Operators Log	(the unit is mounted in the truck and ties to the ignition system, it says touch me, so you touch it, you go)
Cross Match Technologies, Inc.			561.622.1650	561.622.9938	3950 RCA Boulevard, Suite 5001	Palm Beach Gardens	FL	33410	info@crossmatch.com	www.crossmatch.net	Biometrics	ID 500	forensic-quality optical fingerprint identification systems

					Demographic Information									
Company	**Contact**	**Title**	**Phone**	**Fax**	**Address**	**City**	**State**	**Zip**	**E-mail**	**Website**	**Technology Area**	**Product**	**Function/Description**
Cyber Sign Inc.			408.324.1001		180 Montgomery St., Suite 925	San Francisco	CA	94104	info@cybersign.com	www.cybersign.com	Biometrics		signature verification and capture technology
Data Management Inc.	Don Neumann		(510)505-9894	(510)505-9895					sales@csi-monban.com	www.csi-monban.com	Biometrics	Monban Positive Identification System	Biometric fingerprint door access unit. (not for trucks) (there could be some conversion
Digital Persona, Inc.			(650) 261-6070	(650) 261-6079	805 Veterans Boulevard, Suite 301	Redwood City	CA	94063	sales@digitalpersona.com	www.digitalpersona.com	Biometrics	U.are.U Pro	Automated fingerprint authentication that is combined with a password.
exResource									biosecure@exresource.com	www.exresource.com	Biometrics	BioEnter	Authentication for physical door enter and employee tracking.
FingerSec			786-486-5856	810-821-8254	111 Lincoln Rd	Miami Beach	FL	33139	sales@fingersec.com	www.fingersec.com	Biometrics	SmartReader FS100SC	Uses FBI feature extraction method and can be integrated with smart card capability for added security.
Hectrix	Sunita Budhrani	Account Executive	714/573-0494	714/573-0479	18062 Irvine Blvd suite 101	Tustin	CA	92780	sales-us@hectrix.com	www.hectrix.com	Biometrics	ActaTek	Secure Access. Control / Time Attendance using Internet-based Biometrics & Smart Card Technologies.
Identix			(952) 932-0888	(952) 932-7181	5600 Rowland Road	Minnetonka	MN	55343	info@identix.com	www.identix.com	Biometrics	Optical fingerprint sensors	Used for identity verification.
Saflink Corporation	Christina Jin	Project Manager	708-867-7197	843-760-4514	5300 International Blvd	Charleston	SC	29418	cjin@saflink.com	www.saflink.com	Biometrics	BioBox	driver verification
Bulldog Technologies	John Cockburn	CEO	(604) 271-8656	(604) 271-8654	128 - 11180 Coppersmith Pl	Richmond, BC	Canada	V7A 5G8	jcockburn@bulldog-tech.com	www.bulldog-tech.com	**Cargo seal**	Road BOSSTM RB-200	On-Line, real-time wireless cargo security device that attaches to the locking bars on trailers/containers. Integrates with a variety of AVL in-cab products via GPS. If tampered with, a message is sent in real-time to dispatch via GPS and/or driver via pager alert.
Bulldog Technologies	John Cockburn	CEO	(604) 271-8656	(604) 271-8654	128 - 11180 Coppersmith Pl	Richmond, BC	Canada	V7A 5G8	jcockburn@bulldog-tech.com	www.bulldog-tech.com	Cargo seal	Road BOSSTM RB-300	On-Line, real-time wireless cargo security device that attaches to the inside of trailers/containers and monitors multiple access doors on trucks and vans. Integrates with a variety of AVL in-cab products via GPS. If tampered with, a message is sent in real-time to dispatch via GPS and/or driver via pager alert.
Bulldog Technologies	John Cockburn	CEO	(604) 271-8656	(604) 271-8654	128 - 11180 Coppersmith Pl	Richmond, BC	Canada	V7A 5G8	jcockburn@bulldog-tech.com	www.bulldog-tech.com	Cargo seal	Yard BOSSTM RB-100	On-Line, real-time wireless cargo security device that attaches to the locking bars on traliers/containers and is used to monitor door seal integrity and tampering with parked trailers and ocean containers stored in a yard. Works in conjunction with the Bulldog Security Server. Works on motion sensitivity. Can be used as a stand alone system or integrated with an existing alarm system.
CGM Security Systems	Erik Hoffer	President	(800)899-2246	(732)448-1406	223 Churchill Ave	Somerset	NJ	8873	tamperguru@cgmsecuritysolutions.com	www.tamper.com	Cargo Seal	TRAC Door Seals	Self-adhesive seals which are hand applied to a door.
Savi Technologies	Jerry Bredesen	Project Manager	703/317-9254	253/323-5107	615 Tasman Drive	Sunnyvale	CA	94089	jbredesen@savi.com	www.savi.com	Cargo Seal		
CGM Security Systems	Erik Hoffer	President	(800)899-2246	(732)448-1406	223 Churchill Ave	Somerset	NJ	8873	tamperguru@cgmsecuritysolutions.com	www.tamper.com	Cargo seal	Topp Clip Security Solutions	Product provides a 4 prong, solid steel locking mechanism for the generic plastic bands on a pallet. Can be removed using a standard tensioner and crimper.
TeleTouch	Archie Connor	General Manager of 2-way paging	903.535.7800		110 North College Avenue, Suite 200	Tyler	TX	75702	info@teletouch.net	www.teletouch.com	**Employee Emergency**	Life Guard	Allows worker to send a distress signal if they are injured or incapacitated which automatically pinpoints where worker is and brings up their medical history.
Cargo Protectors, Inc.			612.374.3038	612.374.3706	2501 Wayzata Blvd, Suite D	Minneapolis	MN	55405	sales@cargoprotectors.com	www.cargoprotectors.com	**Locks**	Kingpin Lock	
Cargo Protectors, Inc.			612.374.3038	612.374.3706	2501 Wayzata Blvd, Suite D	Minneapolis	MN	55405	sales@cargoprotectors.com	www.cargoprotectors.com	Locks	Pintle Hitch Trailer Lock	
Cargo Protectors, Inc.			612.374.3038	612.374.3706	2501 Wayzata Blvd, Suite D	Minneapolis	MN	55405	sales@cargoprotectors.com	www.cargoprotectors.com	Locks	Roll up door lock	
CGM Security Systems	Erik Hoffer	President	(800)899-2246	(732)448-1406	223 Churchill Ave	Somerset	NJ	8873	tamperguru@cgmsecuritysolutions.com	www.tamper.com	Locks	TS4A Tractor Brake Lock	Lock device that basically cuts the air line from the tractor to the air brakes both tin the tractor and to the trailor.
CGM Security Systems	Erik Hoffer	President	(800)899-2246	(732)448-1406	223 Churchill Ave	Somerset	NJ	8873	tamperguru@cgmsecuritysolutions.com	www.tamper.com	Locks	TS3B Trailer Brake Lock	Locks the air to the brakes rendering them immobile.
CGM Security Systems	Erik Hoffer	President	(800)899-2246	(732)448-1406	223 Churchill Ave	Somerset	NJ	8873	tamperguru@cgmsecuritysolutions.com	www.tamper.com	Locks	SecureT.R.A.C. Self-Wound Void Feature Tape	Applied as normal carton seal tapes and provides physical evidence of tampering through a hidden message revealed when the tape is pealed.
Porter Technologies	Dave Porter	President	(864) 254-9490	(775) 261-5482	1011 West Wade Boulevard	Greer	SC	29650	david@coredefender.com	www.coredefender.com	Locks	CoreDefener	
Power In-Lock	Lowell Werner		800-465-6257	(708) 225-2310	3111 W. 167th Street	Hazel Crest	IL	60429		www.power-in-lock.com	Locks	Power In-Lock	Internal door lock mechanism that requires a driver to gain authorization to open a trailer door. The lock runs off of a battery, solar power or direct power and the locks black box can store up to 2000 events. Events are downloaded to a software program. The Power In-Lock has the ability to integrate with tracking devices and can be accessed with key pads, proximity cards, slide cards, and biometric devices.
Tomal Systems, LLC			(252) 633-4584	(252) 636-5704		New Bern	NC			www.protecsystemone.com	Locks	ProTec System 1	
Transport Security, Inc-ENFORCER®	John Albrecht	VP	(952) 442-LOCK		820 South Pine St	Waconia	MN	55387	enforcer@transportsecurity.com	www.transportsecurity.com	Locks	The ENFORCER®AIR CUFF™	Transport Security, Inc-ENFORCER® manufactures heavy duty locks desined to prevent tractor, trailer, and cargo theft. This includes the Abloy® High Security Padlock. The ENFORCER® King Pin Lock to prevent trailer theft. The ENFORCER®AIR CUFF™ lock designed to prevent truck & trailer theft. Also, a complete line of truck and trailer door locks.
Transport Security, Inc-ENFORCER®	John Albrecht	VP	(952) 442-LOCK		820 South Pine St	Waconia	MN	55387	enforcer@transportsecurity.com	www.transportsecurity.com	Locks		
Wapner Truck Alarm Systems, Inc.			(516) 887-7400		3199 Lawson Blvd.	Oceanside	NY	11572	Sales@truckalarm.com	www.truckalarm.com	Locks	Door	Door lock that reinforces and locks all types of doors.
Agentek, INC	Jeremy Adler	Account Manager	678-393-1808x306	678-393-9950	702 Bombay Lane	Roswell	GA	30076	JeremyA@agentek.com	www.agentek.com	**Software**	Gent Mobile	Agentek serves as front-end for Qualcomm technologies
Air IQ, Inc.	Ann Taylor	VP Sales	905-831-6444	905-831-0567	1099 Kingston Rd, Suite 233	Pickerting, Ontario	Canada	L1V 1B5	ataylor@airiq.com	www.airiq.com	Software	AirIQ OnBoard™	Air IQ OnBOard is the hardware component of Air IQ online and combines the technologies.
Integrated Decision Support Corporation			972-671-0045	972-231-9916	899 Presidential Dr., Suite 117	Richardson	TX	75081	sales@idsc.net	www.idsc.net	Software		

					Demographic Information								
Company	Contact	Title	Phone	Fax	Address	City	State	Zip	E-mail	Website	Technology Area	Product	Function/Description
Maddocks	Shaun Callaghan	Sales Support	604-533-8830	604-533-8562	#211 20644 Eastleigh Crescent	Langley	Canada	V3A 4C4	scalaghan@maddocs.CA	www.maddocks.ca	Software	Truck Mate 4 Windows	Enterprise wide client-server product allowing users to utilize a variety of platforms to mangae shipments, pick up and delivery scheduling, and monitor miles travelled.
Magnasoft Spatial Services, Inc.			(303) 300 4840	(303) 300 2043	2696, S. Colorado Blvd., #270	Denver	CO	80222	bobby@mssglobal.com	www.mssglobal.com	Software		
Maptuit Corp.			(781) 685-4926	(781) 685-4757	35 Corporate Drive - 4th Floor	Boston	MA	1803	info@maptuit.com	www.maptuit.com	Software	FleetNav™	mobile AVLs and has the ability to provide routing and directions.
McLeod Software Corp.	Mark Stephens	Director of Marketing	205-823-5100	205-823-0000	2550 Acton Road / P.O. Box 43200	Birmingham	AL	35243	mark.stephens@mcleodsoftware.com	www.mcleodsoftware.com	Software	LoadMaster	McLeod Software is the leading provider of the most advanced dispatch and accounting transportation management software available to the trucking Industry. McLeod's LoadMaster® product offers a completely integrated transportation management software system that is customizable, and interfaces with most popular mobile communication, mileage and fuel systems. This enterprise-wide solution is based on high performance J2EE technologies.
Object FX Corporation	Kevin Crothers	Project Manager	612-312-2652	612-312-2555	10 2nd Street NE, Suite 400	Minneapolis	MN	55413	kevin.crothers@objectfx.com	www.objectfx.com	Software	Spatial FX	Inegration application with the ability to map, geocode, geofence, provide spatial query and can provide very customized based on customers needs.
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.commm	www.qualcomm.com	Software	Fleet Advisor	
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.commm	www.qualcomm.com	Software	SensorTRACS	
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.commm	www.qualcomm.com	Software	TrailerTRACS	
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.commm	www.qualcomm.com	Software	QTRACS	
Saflink Corporation	Christina Jin	Project Manager	708-867-7197	843-760-4514	5300 International Blvd	Charleston	SC	29418	cjin@saflink.com	www.saflink.com	Software	ESCM system	driver verification/cargo tracking
Saflink Corporation	Christina Jin	Project Manager	708-867-7197	843-760-4514	5300 International Blvd	Charleston	SC	29418	cjin@saflink.com	www.saflink.com	Software		
TeleTouch	Archie Connor	General Manager of 2-way paging	903.535.7800		110 North College Avenue, Suite 200	Tyler	TX	75702	info@teletouch.net	www.teletouch.com	Software	GeoFleet	Custom software to allow monitoring of multiple vehicles on one screen.
TMT Software Company			919.493.4700	919.489.1449	6114 Fayetteville Road, Suite 106	Durham	NC	27713	sales@tmtsoftware.com	www.tmtsoftware.com	Software	TransMan®; Transman/SQL®	
TMW Systems	John Parker	Director, Inside Sales	216-831-6606x204	216-831-3606	21111 Chagrin Blvd	Beahcwood	OH	44122	jparker@tmwsystems.com	www.tmwsystems.com	Software	TMW™ Suite	This software platform supports Windows client/server environments.
TMW Systems	John Parker	Director, Inside Sales	216-831-6606x204	216-831-3606	21111 Chagrin Blvd	Beahcwood	OH	44122	jparker@tmwsystems.com	www.tmwsystems.com	Software	TL2000™	This software platform supports the use of the AS/400.
TrackStar	Terri Recknor	President	315-721-0931	315-721-0934	8382 Seneca Trunpike	New Hartford	NY	13413	terrir@trackstar.com	www.trackstar.com	Software	Track Start Fleet Manager Software	Software that supports the Track Star ® Safety and Security System
UPS Logistics Technologies			410.847.1900	410.847.6246	849 Fairmount Avenue	Baltimore	MD	21286	market@upslogistics.com	www.roadnet.com	Software	Territory Planner ™	Uses historical route data to plan the best routes and delivery times.
UPS Logistics Technologies			410.847.1900	410.847.6246	849 Fairmount Avenue	Baltimore	MD	21286	market@upslogistics.com	www.roadnet.com	Software	Roadnet 5000™	Uses algorithms and street-level routing to improve routing efficiency.
ALK Technologies, INC	George Cummings	Senior Account Executive	800-377-6453x123	609-683-0290	1000 Herrontown Road	Princeton	NJ	08540	cummings@alk.com	www.pcmiler.com	Software	PC*Miler	Routing, Mileage, and Mapping Software.
ALK Technologies, INC	George Cummings	Senior Account Executive	800-377-6453x123	609-683-0290	1000 Herrontown Road	Princeton	NJ	08540	cummings@alk.com	www.pcmiler.com	Software	PC*Miler Hazmat	
ALK Technologies, INC	George Cummings	Senior Account Executive	800-377-6453x123	609-683-0290	1000 Herrontown Road	Princeton	NJ	08540	cummings@alk.com	www.pcmiler.com	Software	Fleet Commander	
ALK Technologies, INC	George Cummings	Senior Account Executive	800-377-6453x123	609-683-0290	1000 Herrontown Road	Princeton	NJ	08540	cummings@alk.com	www.pcmiler.com	Software	CoPilot Truck	
Telcontar			415-908-4400		612 Howard Street, Suite 300	San Francisco	CA	94105	marketing@telcontar.com	www.telcontar.com	Software	Universal Telematics Server™	Software that can be integrated with mobile tracking devices.
Advanced Productivity Computing			952-432-2000	952-432-1222	14690 Galaxie Avenue, Suite 114	Apple Valley	MN	55124		advancedproductivity.com/fleettracking.asp	**Vehicle Tracking**	Coyote	Tracks truck through 2 minute updates.
Advanced Productivity Computing			952-432-2000	952-432-1222	14690 Galaxie Avenue, Suite 114	Apple Valley	MN	55124	bob@networkinv.com	advancedproductivity.com/fleettracking.asp	Vehicle Tracking	Roadrunner	Uses a pocket PC to enhance Coyote with instant messaging.
Advanced Productivity Computing			952-432-2000	952-432-1222	14690 Galaxie Avenue, Suite 114	Apple Valley	MN	55124	bob@networkinv.com	advancedproductivity.com/fleettracking.asp	Vehicle Tracking	Skyrunner	Tracks vehicle via satellite at a configurable rate.
Advanced Productivity Computing			952-432-2000	952-432-1222	14690 Galaxie Avenue, Suite 114	Apple Valley	MN	55124	bob@networkinv.com	advancedproductivity.com/fleettracking.asp	Vehicle Tracking	Skyhawk	Less-than-real-time satellite tracking configurable between once per hour to once per day.
Aether Systems, Inc.	Michael Brown	V.P., Product Marketing	972-301-2702	410-654-6554	11460 Cronridge Drive	Owings Mills	MD	21117	mbrown@aethersystems.com	www.aethersystems.com	Vehicle Tracking	20/20V	20/20V uses GPS technology to track vehicles through a web-based application. It has the ability to locate vehicles, map current and historical locations, geo-fencing, address locator, e-mail notification, and records starts and stops.
Aether Systems, Inc.	Michael Brown	V.P., Product Marketing	972-301-2702	410-654-6554	11460 Cronridge Drive	Owings Mills	MD	21117	mbrown@aethersystems.com	www.aethersystems.com	Vehicle Tracking	MobileMax	MobileMax utilizes both satellite and terrestrial tracking. It has GPS standard, built-in distress alert, street-level mapping, proximity notifications, real-time messaging, and disptch messaging.
Air IQ, Inc.	Ann Taylor	VP Sales	905-831-6444	905-831-0567	1099 Kingston Rd, Suite 233	Pickerting, Ontario	Canada	L1V 1B5	ataylor@airiq.com	www.airiq.com	Vehicle Tracking	AirIQ OnLine™	Uses web-based GPS tracking with satellite and terrestrial technology for a comprehensive user end product that is capable of mapping, unlock a door, etc.
AirLink, Inc			(510) 226-4200	510-226-4299	472 Kato Terrace	Fremont	CA	94539	info@airlink.com	www.airlink.com	Vehicle Tracking	AirLink Tracking System	Terrestrial tracking.
AtRoad	Norm Geotzke - NLG Enterprises; 651-457-4149		(510) 668-1638	(510) 870-1444	47200 Bayside Parkway	Fremont	CA	94535		www.atroad.com	Vehicle Tracking	MobileForms	Handheld interface allows remote collection and transmission of field data. It reads bar codes, allows two-way messaging, has ability to create and send custom data forms.
AtRoad	Norm Geotzke - NLG Enterprises; 651-457-4149		(510) 668-1638	(510) 870-1444	47200 Bayside Parkway	Fremont	CA	94535		www.atroad.com	Vehicle Tracking	iTM™ Internet Trailer Manager	Self-powered unit uses GPS to determine and report trailer location, tethered or untethered status, and has an optional door status sensor.
Avel-Tech			(450) 682-6262	(450) 682-8117	2525 Daniel Johnson Boulevard, Suite 300	Laval, Quebec	Canada	H7T 1S9	info@avel-tech.com	www.avel-tech.ca	Vehicle Tracking	Avel-Net	Tracking enabled with either terrestrial or satellite and complete with mapping capabilities.
Burdilla Lanser Technologies LLC	Graham Fraser	Director	(530) 885-2550	(530) 885-1808	115 Pine Street	Auburn	CA	95603	gfraser@trakwhere.com	www.trakwhere.com	Vehicle Tracking	Vehicle Location/Tracking	
Cabit Systems			416-916-2591	416-282-3665	4117 Lawrence Ave E, Suite 203	Toronto, Ontario	Canada	M1E 2S2	info@cabit.com	www.cabit.com	Vehicle Tracking	Cabit OSB	Tracking with both terrestrial and satellite tracking as well as 2-way messaging.
Cheetah Software Systems	David Linville	Director of Sales	805-373-7111	805-373-7112	200 North Westlake Blvd Ste 200	Westlake Village	CA	91362	dlinville@cheetah.com	www.cheetah.com	Vehicle Tracking	Cheetah Freight	Terrestrial based sysetm uses GPS and cell phones to provide tracking as well as two-way messaging. User is provided with mapping capabilities.
Cloudberry Wireless Services			858-677-9950	858-677-9959	11353 Sorrento Valley Rd	San Diego	CA	92121	sales@cbwireless.net	www.cloudberry.com	Vehicle Tracking	TerraTrak	GPS tracking with internet based user mapping capabilites.
Cloudberry Wireless Services			858-677-9950	858-677-9959	11353 Sorrento Valley Rd	San Diego	CA	92121	sales@cbwireless.net	www.cloudberry.com	Vehicle Tracking	TerraTrak+	TerraTrak capabilities plus a pocket pc for 2-way messaging.

					Demographic Information								
Company	Contact	Title	Phone	Fax	Address	City	State	Zip	E-mail	Website	Technology Area	Product	Function/Description
Cloudberry Wireless Services			858-677-9950	858-677-9959	11353 Sorrento Valley Rd	San Diego	CA	92121	sales@cbwireless.net	www.cloudberry.com	Vehicle Tracking	DualTrak+	Combination terrestrial and satellite GPS tracking with 2 way messaging.
CSI Wireless			403-259-3311	403-259-8866	4110 9th St SE	Calgary, Alberta	Canada	T2G 3C4	info@csi-wireless.com	www.csi-wireless.com	Vehicle Tracking	CSI Fleet-Link	Satellite and terrestrial tracking.
EarthTRAK			615-391-2255	615-467-2675	2727 Old Elm Hill Pike	Nashville	TN	37214	operations@earthtrak.com	www.earthtrak.com	Vehicle Tracking	EarthTRAK™	GPS terrestrial fleet tracking.
Fleetilla	Dennis Reno		(734) 362-3260		1650 West Jefferson	Trenton	MI	48183	info@fleetilla.com	www.fleetilla.com	Vehicle Tracking	FL 1700	FL1700 is a tracking and communication system that provides real-time location updates using GPS. Coverage Sensing™ provides reliability in ou lying cellular areas. Provides event and exception notifications, automatic and on-demand location updates, motion detection, web accessible, option to include keyboard for driver alert and receipt confirmation, operating metrics reporting, geo-fencing, different antenna configurations, and serial interface to external accessories.
Fleetilla	Dennis Reno		(734) 362-3260		1650 West Jefferson	Trenton	MI	48183	info@fleetilla.com	www.fleetilla.com	Vehicle Tracking	FleetVOX	Provides updates via cellular communications.
GE TIP			1-800-333-2030						info@tiptrailers.com	www.tiptrailers.com	Vehicle Tracking	GE Veriwise	Satellite tracking.
Global 2-Way	Greg Harper	Product Manager	239-642-2083 ext. 270	239-642-9283	628-A Bald Eagle Drive	Marco Island	FL	34145	gregharper@global2way.com	www.global2-way.com	Vehicle Tracking	Global T-Fleet	Utilizes GPS technology through terrestrial means, as well as FM and digital high-frequencies, to provide automatic event reporting and 2-way communications. Drivers operate off of a mobile terminal, and dispatchers have ability to map locations. There is also an emergency alert for drivers.
GPS Management									info@gpsmanagement.com	www.gpsmanagement.com	Vehicle Tracking	Real Time D-1000 system	Product provides GPS tracking technology with cellular communications.
GPS Management									info@gpsmanagement.com	www.gpsmanagement.com	Vehicle Tracking	Non Real Time System P-3000	Stores information such as location, speed, etc. for downloading and viewing at a later date.
Ida Corporation			701-280-1122	218-233-1886	1345 Main Ave	Fargo	ND	58103	info@idaco.com	www.idaco.com	Vehicle Tracking	TrakIt™	GPS enabled cellular phone tracking and also provides text messaging.
Insight USA	John Eller	President	(301) 866-1990	(301) 866-1992	23330 Cottonwood Parkway, Suite 333	California	MD	20619	johneell@mds-inc.com	www.mds-inc.com	Vehicle Tracking	StreetEagle	GPS satellite tracking with routing capabilities.
InterTrak			1-866-346-3631		PO Box 830	Frisco	TX	75034	sales@trackmenow.com	www.trackmenow.com	Vehicle Tracking	InterTrak	Satellite and terrestrial tracking.
IRD, Inc			303.355-5998	303.426-8937	702 43rd St East	Saskatoon, SK	Canada	S7K 3T9	info@irdinc.com	www.irdinc.com	Vehicle Tracking	Automatic Vehicle Compliance Monitoring System	Satellite tracking.
Lorantec Systems, Inc.	Jim Schreitmueller	Vice President, Sales & Marketing	925/552-7101	952/552-7101	1052 Pendleton Ave	Sunnyvale	CA	94087	jschreitmueller@lorantec.com	www.lorantec.com	Vehicle Tracking	Vehicle Location/Tracking	satellite tracking, In-transit visibility (ITV), asset tracking
Metler Toledo	Felix Klebe	Business Manager	614-438-4444		1150 Dearborn Dr.	Worthington	OH	43085	felix.klebe@mt.com	www.mt.com	Vehicle Tracking	Video Capture	Satellite tracking.
Minor Planet			972-301-2100	972-301-2403	1155 Kas Drive	Richardson	TX	75081	info@minorplanetusa.com	www.minorplanetusa.com	Vehicle Tracking	Vehicle Management Information	Satellite tracking.
Mobilearia, Inc.	Karl Mehta	Vice President	650-237-4405	650-937-1078	800 West El Camino Real, Suite 240	Mountain View	CA	94040	info@mobilearia.com	www.mobilearia.com	Vehicle Tracking	TruckSecure™	Suite of technologies for trucking security including satellite vehicle tracking, wireless key fob panic button, route restrictions, and vehicle disablement.
Mobilearia, Inc.	Karl Mehta	Vice President	650-237-4405	650-937-1078	800 West El Camino Real, Suite 240	Mountain View	CA	94040	info@mobilearia.com	www.mobilearia.com	Vehicle Tracking	FleetOutlook™	Satellite tracking using the Delphi Truck PC which is disguised as a radio.
Network Innovations			1(800) 848-0326		1851 Swede Gulch Road	Golden	CO	80401	bob@networkinv.com	www.networkinv.com	Vehicle Tracking	EasyTrack Mini-C System	
Northwest Nuclear, LLC	Steve Miller	Sales Engineer	256-404-4929	770-932-9621	3455 Summit Trail	Cummings	GA	30041	yankengr@charter.net	www.seekernetinc.com	Vehicle Tracking		Terrestrial and satellite tracking.
Orbcomm			703.433.6300	703.433.6400	21700 Atlantic Boulevard	Dulles	VA	20166	sales.contact@orbcomm.com	www.orbcomm.com	Vehicle Tracking	Orbcomm Subscriber Communicators	Satellite tracking.
Pana-Pacific	Deborah Cameron	Director, TruckPC Marketing	615-776-4159	615-566-1007	908 Bluff Road	Brentwood	TN	37027	dlcameron5@comcast.net	www.panapem.com	Vehicle Tracking	Truck Productivity Computer	The computer allows for tracking, 2 way messaging, and vehicle monitoring - the device is on-board, but is disguised as an AM/FM radio Cd player. Tracking technology from Mobilearia is used which includes both satellite and terrestrial tracking capabilities as well as wireless LAN.
PeopleNet Communications Corporation	Cheryl Wallace	Sales	888-346-3486	(952) 368-9320	1107 Hazeltine Blvd, Suite 350	Chaska	MN	55318	cwallace@peoplenet.com	www.peoplenetonline.com	Vehicle Tracking	PeopleNet g2X™	Uses GPS and wireless satellite to track trucks, predict ETA's, and determine vehicle speeds. Has the ability through PACOS to perform exception-based messaging through geofencing.
PeopleNet Communications Corporation	Cheryl Wallace	Sales	888-346-3486	(952) 368-9320	1107 Hazeltine Blvd, Suite 350	Chaska	MN	55318	cwallace@peoplenet.com	www.peoplenetonline.com	Vehicle Tracking	Metro™	Uses GPS and wireless satellite to track trucks, predict ETA's, and determine vehicle speeds. Has the ability through PACOS to perform exception-based messaging through geofencing.
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.comm	www.qualcomm.com	Vehicle Tracking	MVPc	Satellite tracking.
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.comm	www.qualcomm.com	Vehicle Tracking	OmniTRACS	Satellite tracking.
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.comm	www.qualcomm.com	Vehicle Tracking	OmniExpress	Terrestrial tracking.
Qualcomm	Derrick Vercoe	Director of Operations	858-651-6413	858-658-1596	5775 Morehouse Drive	San Diego	CA	92121	dvercoe@qualcom.comm	www.qualcomm.com	Vehicle Tracking	T2	Satellite tracking.
Safefreight Technologies	Shauna Peets	Communications Director	780.421.9055	780.421.9011	4600 Touchton Rd, Building 100, Suite 303	Jacksonville	FL	32246	speets@safefreight.com	www.safe-freight.com	Vehicle Tracking	Vanguard, Security Guard	Terrestrial and satellite tracking.
Safefreight Technologies	Shauna Peets	Communications Director	403-202-2467		4507-49 St NW	Calgary	Canada	T3A 1X4	speets@safefreight.com	www.safefreight.com	Vehicle Tracking		Terrestrial and satellite tracking.
Sage Quest	Bruce Del Vecchio	VP Sales & Marketing	888-837-7243 ext228	216-765-0936	23550 Commerce Park	Beachwood	OH	44122	bdelvecchio@sage-quest.com	www.sage-quest.com	Vehicle Tracking		Terrestrial tracking.
Satellite Security Systems of North America			619-574-1452	619-574-6521					sales@satsecurity.com	www.satsecurity.com	Vehicle Tracking	FleetGuard™	GPS tracking utilizes satellite technology and two-way paging to track fleets.
Telemisphere LLC	John Carlin	President	(440) 582-8839		1128 W. Pleasant Valley Rd.-108	Parma	Ohio	44134-6711	Jcarlin@telemisphere.com	www.telemisphere.com	Vehicle Tracking	Vehicle Location/Tracking	Offers highly sensitive GPS devices and networks that cover the entire US, allowing devices to roam from Terrestrial networks to a Ubiquitous overlay Network offered by our Supplier Space Data Corp. Devices are quoted as quantity one. Airtime or usage depends on the number of times device needs to be located in a month and is also quoted as quantity 1 pricing. The devices are capable of carrying data back from many different types of sensors required in the vehicle.
TeleTouch	Archie Connor	General Manager of 2-way paging	903.535.7800		110 North College Avenue, Suite 200	Tyler	TX	75702	info@teletouch.net	www.teletouch.com	Vehicle Tracking	Tracker AVL	Uses GPS to monitor and track trucks through cellular, or can combine messaging technologies via satellite.
Telogis	Steven Rabago; Richard Kooyenga	CEO; Senior Sales Executive	949-646-6637	866-422-4096	1041 W.18th St.Suite A101	Costa Mesa	CA	92627-6313	richard.kooyenga@telogis.com	www.telogis.com	Vehicle Tracking	OnTrack2	OnTrack2 provides vehicle location data, mapping software and geofencing, as well as functional software such as mileage reports and other ROI contributing factors. It has the ability to integrate with other technologies, and has a data port for laptop access. Web-based access allows the user to manually locate trucks or location reports are generated every 10 minutes.

					Demographic Information								
Company	**Contact**	**Title**	**Phone**	**Fax**	**Address**	**City**	**State**	**Zip**	**E-mail**	**Website**	**Technology Area**	**Product**	**Function/Description**
TrackStar	Terri Recknor	President	315-721-0931	315-721-0934	8382 Seneca Trunpike	New Hartford	NY	13413	terrir@trackstar.com	www.trackstar.com	Vehicle Tracking	Track Star Safety and Security Sysetm	Terrestrial based AVL system that tracks using GPS. Positions for such events as panic buttons, theft alarms
Transcore	Bob Frank	Fleet and Asset Management Services	508.393.2762	508.393.5702	19111 Dallas Parkway, Suite 300	Dallas	TX	75287	bob.frank@transcore.com	www.transcore.com	Vehicle Tracking	Smartwatch	
Trimble	Kimberly DeCoste	Sales	408-481-8000		645 N Mary Ave	Sunnyvale	CA	94088	kimberley_decoste@trimble.com	www.trimble.com	Vehicle Tracking	Telvisant Fleet Management Services	Web-based satellite/terrestrial combination vehicle tracking with additional sensor capability.
Vericom Technologies	John Bjorn	President	410-381-5707	410-381-7417	9881 Broken Land Pkwy, Suite 400	Columbia	MD	21046	jbjorn@vericomtech.com	www.vericomtechnologies.com	Vehicle Tracking	Fleet Management	Satellite tracking.
Vistar	Ann Kelly	Director of Marketing	613-591-0100	613-230-0820	427 Laurier Ave. W, Suite 1410	Ontario	Canada	K1R 7Y2	akelly@vistar.ca	www.vistar.ca	Vehicle Tracking		Satellite tracking.
Waveburst Communications, Inc.			408-996-3344	408-252-8780	1777 Saratoga Ave	San Jose	CA	95129	sales@waveburst.com	www.waveburst.com	Vehicle Tracking		Satellite and terrestrial tracking.
Xata	Tom Fleece		612/867-2753	952-894-2463	151 E Cliff Road, Suite 10	Burnsville	MN	55337		www.xata.com	Vehicle Tracking		Satellite tracking.
Aeris.net			408-557-1900		1245 S. Winchester Blvd	San Jose	CA	95128	info@aeris.net	www.aeris.net	Vehicle Tracking		Terrestrial tracking.
PowerLoc Technologies, Inc.			905-764-3701	905 764 3690	30 Leek Crescent, Suite 103	Richmond Hill, Ontario	Canada	L4B 4N4	info@powerloc.com	www.powerloc.com	Vehicle Tracking	VLD	Terrestrial tracking.
V-TRAC Systems, INC	Lee Moore	President	877-273-7434	877-273-7164	230 Colfax Avenue	Grass Valley	CA	95945	lee@vtracsystems.com	www.vtracsystems.com	Vehicle Tracking	V-Link 2	Vehicle tracking device uses GPS and terrestrial means to perform 2-way messaging.

	Possible Applications																								Current Operations			Pricing				
Company	Satellite Tracking	Cellular Phones or Paging Service	Terrestrial Tracking	Automated Collision Notification	Trailer Tracking	Untethered Trailer Tracking	Keypad Personnel Authentication	Trailer Securement	Biometric Authentication	Driver Authentication	Asset Management	Asset Tracking	Mapping	Remote Vehicle Disabling	Inventory Management	Web-based Shipment Tracking	Radio Frequency Identification Tag	Out of Route Mapping System or Alert	Electronic Cargo Seals	Mechanical Cargo Seals	In-Vehicle Mounted Computer	In-Vehicle Communications	Integration Software	Consultant Services	Others, please describe	Average Operation Size	Type of Operation	Market Expansion	Per Unit Base Cost	Per Unit + Installation	Maintenance Costs	Recurring Service Costs	Notes
Vericom Technologies								x	x	x	x	x		x		x	x		x	x				x	See Note								Flexible, recyclable, standards based soultion for container security
Zonar									x	x																100 + power units	CVO - hazmat, t	possibly rail	$300-RFID tags and readers	Customers are able to perform themselves, and not an involved process.		Varies dependent on fleet size.	
Engineered Inerting Systems							X - smartcard and employee code			x	x	x					x					x	X - See Note 1	x	See Note 2								1- has ability to integrate with HOS and maintenance software, 2-security sweeps and electronic EVIRs
Aether Systems, Inc.																									See Note	Aether serves a variety of trucking company sizes	Aether serves a variety of trucking company sizes		TrailerMax has a $350 to $400 per unit price.	Average installs range from $100-$125 per units.		Service fees range from $4.99 to to $14.99 per unit.	Material inhibits explosiveness of materials for tanker trucks and others.
Aether Systems, Inc.	x				x	x		x					x													Aether serves a variety of trucking company sizes	Aether serves a variety of trucking company sizes		GeoLogic prices range between $450 to $500 per unit.	Average installs range from $100-$125 per units.		Service fees range from $10 to $15 per unit per month.	
Aircept	x				x	x					x	x																					
Datacom																																	
Fleetilla																												$469.00 - See Note 1			See Note 2	1- Includes wiring harness, battery bracket and combo antenna. 2-One update per day is $8 per month, and two updates per day is $11 per month. Additional two way updates are available at 0.30 per use. Custom plans are also available.
General Electric	x				x	x		x				x	x					x										$440	$575		$10-13.50	
GPS Management	x					x																											
Intermodal Security Devices			x										x															<$400.00	<400.00	Nil	Nil	
Lat-Lon, LLC										x		x	x	x				x								100+	Road Shipper	100+ (containe	$500 - 1,500	$500 - $1,500	0	$8 - $15 per month	
Lat-Lon, LLC		x	x		x	x					x	x	x			x			x				x			100+	Rail Shipper	3000+	$700 - $2,000	$700 - $2,000	0	$8 - $15 per month	
Mobilearia, Inc.		x	x		x	x					x	x	x			x			x				x									
PAR Technologies																	x																
Qualcomm												x														1000 trailers	For-hire and Private fleets with Vans and reefers	Fleets with Tankers	$139 Van/ $189 Refer	$60.00		See Note	averages 30 cents per month over and above the OmniTRACS monthly costs
SkyBitz			x		x					x	x	x						x						x				$375-$440	$30-35.20		$7.50-$15	
SkyBitz	x				x	x						x	x			x												$375-$440	$30-35.20		$7.50-$15	
SkyBitz	x				x							x	x			x												$375-$440	$30-35.20		$7.50-$15	
TeleTouch					x							x	x																				
Terion	x				x							x	x			x																	
Terion					x																												
TrackStar																									X - Cargo Sen	See Note 1	See Note 2		See Note 3			See Note 4	1-This product is currently being utilized by small to mid-sized carriers. 2-TrackStart currently provides services for coin carriers, executive protection, hazmat carriers and Latin America. 3-The per unit cost of this product is $495 and can differ depending on quantity purchased. 4-Average monthly fees run from $7.70 and up.
V-TRAC Systems, INC			x			x							x																				
AcSys Biometrics Corporation	x		x										x																				
ActivCard									x																								
AuthenTec									x																	See Note 1	OEM, ODM	See Note 2	$6 and up in volume				1- they partner with hardware manufacturers and vendors, not end product at all, 2-They evaluate new markets and trends
Biocentric Solutions Inc.									x																								
Bioidentix									x																								
Bio-Key International																																	
Cogent Systems									x																								
Compu-Trol Technologies Inc.									x	x																na	na	na	– $1000	na	na	na	
Cross Match Technologies, Inc.									x																								

	Possible Applications																								Current Operations			Pricing				
Company	Satellite Tracking	Cellular Phones or Paging Service	Terrestrial Tracking	Automated Collision Notification	Trailer Tracking	Untethered Trailer Tracking	Keypad Personnel Authentication	Trailer Securement	Biometric Authentication	Driver Authentication	Asset Management	Asset Tracking	Mapping	Remote Vehicle Disabling	Inventory Management	Web-based Shipment Tracking	Radio Frequency Identification Tag	Out of Route Mapping System or Alert	Electronic Cargo Seals	Mechanical Cargo Seals	In-Vehicle Mounted Computer	In-Vehicle Communications	Integration Software	Consultant Services	Others, please describe	Average Operation Size	Type of Operation	Market Expansion	Per Unit Base Cost	Per Unit + Installation	Maintenance Costs	Recurring Service Costs	Notes
Cyber Sign Inc.									X																							
Data Management Inc.									X																	banks, private developments		1200				owned by toyota in Japan. Now
Digital Persona, Inc.									X																3-4 people to several million people	banks, offices, etc.		$99				would have to be built in a custom way. Could the ignition be controled by an electoronic systme
exResource									X																							
FingerSec									X																							
Hectrix									X																							
Identix									X																							
Saflink Corporation									X																			$800.00	user install	user maintain		
Bulldog Technologies									X	X						X									1 - 500+	See Note 1		$1,495 (see note 2)	Customer Install	$0	Batteries at $85	1-Tractor-trailer trucking companies, Yard facilities, Private fleets, Owner/Operators, 2-per unit including BOSSTM Pager or GPS Interconnect, Battery Pack, Attachment Clamp
Bulldog Technologies	X	X	X		X	X	X	X			X	X	X	X			X	X	X	X	X	X		X	1 - 500+	See Note 1		$1,295 (see Note 2)	Customer Install	$0	Batteries at $85	1- Originally built for trucks and delivery vans with roll-up doors. Couriers, deliver companies. 2-per unit including BOSSTM Pager or GPS Interconnect, Battery Pack, Door Contact.
Bulldog Technologies	X	X	X		X	X	X	X			X	X	X	X			X	X	X	X	X	X		X	1 - 2,000	See Note 1		$1,195 (See Note 2)	Customer Installed	$0	Batteries at $85	1- Container storage facilities, contianer handling facilities, trailer storage yards. 2-per unit including Battery Pack and Attachment Clamp
CGM Security Systems						X	X	X			X			X				X		X				X				See Note				1000=$1.59 per seal; 2500-5000=$1.45; 5,000-10,000=$1.10; 10,000-25,000=$.945; 25,000-50,000=.845; 50,000-10,000=$.795
Savi Technologies																									X- (See Note)							Self-adhesive door seal.
CGM Security Systems																												See Note				Carton quatity - 1-9=$545; 10-25=$450; 26-125=$394; 126-250=$356; >250=$338
TeleTouch																				X												
Cargo Protectors, Inc.	X		X																													
Cargo Protectors, Inc.																									Mechanical Door Lock							
Cargo Protectors, Inc.																									Mechanical Door Lock							
CGM Security Systems																									Mechanical Door Lock			See Note				1-10=$195; 11-25=$185; 26-50=$180; >50=$175
CGM Security Systems																									Brake Lock			See Note				1-10=$333 each; 11-25=$298; 26-50=$288; 51-250=$265; 251+=$244
CGM Security Systems																									Trailer Brake							
Porter Technologies																									Tamper tape							
Power In-Lock																												See Note 1	See Note 2		There is no monthly charge, as all events are downloaded into software by the user.	1- $595 - Complete with the lock, black box and key fob. 2-Installation is included, and on average will take approximately one hour, dependent on how hidden it is.
Tomal Systems, LLC																												See Note				$432 per unit or $588 per unit w/ pager
Transport Security, Inc-ENFORCER®																																
Transport Security, Inc-ENFORCER®																																
Wapner Truck Alarm Systems, Inc.	X				X		King PIN LOCK				X					X	X	Abloy® Electronic seals														
Agentek, INC																																
Air IQ, Inc.																						X										
Integrated Decision Support Corporation	X		X		X	X		X			X	X	X	X	X	X		X			X		X	X								

	Possible Applications																								Current Operations			Pricing				
Company	Satellite Tracking	Cellular Phones or Paging Service	Terrestrial Tracking	Automated Collision Notification	Trailer Tracking	Untethered Trailer Tracking	Keypad Personnel Authentication	Trailer Securement	Biometric Authentication	Driver Authentication	Asset Management	Asset Tracking	Mapping	Remote Vehicle Disabling	Inventory Management	Web-based Shipment Tracking	Radio Frequency Identification Tag	Out of Route Mapping System or Alert	Electronic Cargo Seals	Mechanical Cargo Seals	In-Vehicle Mounted Computer	In-Vehicle Communications	Integration Software	Consultant Services	Others, please describe	Average Operation Size	Type of Operation	Market Expansion	Per Unit Base Cost	Per Unit + Installation	Maintenance Costs	Recurring Service Costs	Notes
Maddocks																																
Magnasoft Spatial Services, Inc.																							X									
Maptuit Corp.																																
McLeod Software Corp.	X		X		X	X					X	X	X			X		X			X		X	X	ument Ima	150 trucks	For-hire truckload and private carriers		Custom	Custom	Optional	None	
Object FX Corporation																													Costs will be based on a variety of variables.				
Qualcomm												X	X					X					X			200 trucks	Private fleets		Site license ($	None	15%	+$15.00 over OmniTRACS/OmniExpress costs	
Qualcomm	X		X		X					X	X	X	X					X			X	X	X	X		200 trucks	For-hire fleets		$10,000 Fleet	None	15%		
Qualcomm											X	X											X	X		1000 trailers	For-hire and Priv	Fleets with Tar	$10,000 Fleet	None	15%		
Qualcomm			X		X			X			X	X	X											X		200 trucks	For-hire and Private fleets		$35,000 Fleet	None	15%		
Saflink Corporation																												Server Component -	$5,000.00	site dependent		18%/year	Software only
Saflink Corporation									x	x						X												Site Software	$495	site dependent		18%/year	Software only
TeleTouch																																
TMT Software Company																							X									
TMW Systems																							X									
TMW Systems																							X									
TrackStar																							X			See Note	See Note 2		$995 software cost.				1- Track Star has had success with many different carriers, but has seen small to medium-sized carriers the most. 2- Operations ranging from hazmat, armored vehicles, executive protection and many carriers in Latin America.
UPS Logistics Technologies													X					X														
UPS Logistics Technologies													X					X					X									
ALK Technologies, INC													X										X									
ALK Technologies, INC																							X									
ALK Technologies, INC																																
ALK Technologies, INC																																
Telcontar																																
Advanced Productivity Computing																							X									
Advanced Productivity Computing			X										X																			
Advanced Productivity Computing			X										X																			
Advanced Productivity Computing	X											X	X																			
Aether Systems, Inc.	X											X	X													See Note 1	See Note 1		$499	See Note 2		See Note 3	1- Aether serves a variety of trucking company sizes. 2- Installation costs from a third-party provider can be approximately $50-75. 3- Service fees range from $19.95 to $39.95 per unit per month.
Aether Systems, Inc.	X		X										X			X		X								See Note 1	See Note 1		See Note 2	See Note 3		See Note 4	1- Aether serves a variety of trucking company sizes. 2- Prices range between $1,800 and $2,100. 3- Installation costs can cost $125. 4- Service fees range from $35-$50 per unit per month.
Air IQ, Inc.	X		X										X																			
AirLink, Inc	X											X	X	X																		
AtRoad																																
AtRoad																																
Avel-Tech					X	X		X																								
Burdilla Lanser Technologies LLC						X								X																		
Cabit Systems	X		X										X																			
Cheetah Software Systems	X		X										X																$20 set-up fee per phone.			Subscription fees range from $10-$20 per phone per month.	
Cloudberry Wireless Services		X	X										X																			
Cloudberry Wireless Services			X										X																			

	Possible Applications																								Current Operations			Pricing				
Company	Satellite Tracking	Cellular Phones or Paging Service	Terrestrial Tracking	Automated Collision Notification	Trailer Tracking	Untethered Trailer Tracking	Keypad Personnel Authentication	Trailer Securement	Biometric Authentication	Driver Authentication	Asset Management	Asset Tracking	Mapping	Remote Vehicle Disabling	Inventory Management	Web-based Shipment Tracking	Radio Frequency Identification Tag	Out of Route Mapping System or Alert	Electronic Cargo Seals	Mechanical Cargo Seals	In-Vehicle Mounted Computer	In-Vehicle Communications	Integration Software	Consultant Services	Others, please describe	Average Operation Size	Type of Operation	Market Expansion	Per Unit Base Cost	Per Unit + Installation	Maintenance Costs	Recurring Service Costs	Notes
Cloudberry Wireless Services			X										X																			
CSI Wireless	X		X										X																			
EarthTRAK																																
Fleetilla			X										X															$429.00 - See Note 1			See Note 2	1- Includes wiring harness and combo antenna. Optional keypad for $60.00. 2- Monthly plans range from $11 to $44 plus additional charges for one way and two way updates ranging from $0.15 to $0.30 per use.
Fleetilla	X											X	X					X														
GE TIP	X																															
Global 2-Way																									Average operation size ranges greatly.	There product has been utilized by all different types of operations.	They target fleets over 40 power units.	See Note 1			See Note 2	1- New hardware costs $1,895; re-certified hardware costs $1,000. 2- Depending on customer configuration, monthly fees range from $25-$55 per unit per month.
GPS Management			X										X					X			X	X										
GPS Management			X										X																			
Ida Corporation			X										X																			
Insight USA		X	X									X	X															See Note				Pricing differs but they do offer leasing, long-term and short-term purchase plans.
InterTrak	X												X					X														
IRD, Inc																																
Lorantec Systems, Inc.	X		X	X	X	X						X	X			X		X						X			See Note 1		See Note 2	See Note 3	See Note 4	See Note 5	1- Ocean carrier, trucking company, railway, heavy equipment. 2- $299 and up, subject to configuration and quantity. 3- Self installable or Cost + 15%. 4- Replacement battery for untethered application, subject to desired operational duration, e.g. 90 days-5 yrs.). 5- Monthly service fee as low as $5 for two reports per asset tracked per day.
Metler Toledo																																
Minor Planet																																
Mobilearia, Inc.																																
Mobilearia, Inc.	X									X			X					X														
Network Innovations	X									X			X					X														
Northwest Nuclear, LLC	X											X	X																			
Orbcomm																																
Pana-Pacific																																
PeopleNet Communications Corporation	X		X								X		X					X							They provide services to a range of operation sizes.	majority are midrange to longhaul general frieght haulers.		See Note				PeopleNet operates off of a lease program which ranges between $69 and $89 per month per unit. This can differ based on customer configurations.
PeopleNet Communications Corporation	X		X										X					X			X				They provide services to a range of operation sizes.	See Note						provide services to all types, but majority are midrange to longhaul general frieght haulers.
Qualcomm	X		X										X					X			X				200 trucks	Private fleets		$1,000.00	None	15%		
Qualcomm																									200 trucks	For-hire and Private fleets		$2,275.00	$300.00	15%	$50.00 per month	
Qualcomm	X					X			X	X	X	X	X	X	X			X			X	X	X	X	200 trucks	For-hire and Private fleets	Service Fleets	$1,290.00	$170.00	15%	$50.00 per month	
Qualcomm		X	X			X			X	X	X	X	X	X	X			X			X	X	X	X	1000 trailers	For-hire and Private fleets with Vans and reefers	Fleets with Tankers	not commericaly available	not commercialy available		not commercialy available	
Safefreight Technologies			X		X	X		X			X	X	X		X			X	X	X	X	X	X	X								
Safefreight Technologies																																
Sage Quest																																
Satellite Security Systems of North America																																
Telemisphere LLC	X	X	X	Possible	X	X						X	X	X				X									Carrier/ASP	US Ubiquitous coverage, Canada, MEX	$399	n/a		$7+ depending on usage	
TeleTouch	X												X																			
Telogis	X		X										X												See Note 1	See Note 2	See Note 3	See Note 4	$595+75	None	See Note 5	1- OnTrack2 has a customer base ranging from a few power units to some very large trucking corporations. 2- OnTrack2 primarily serves urban and metropolitan based fleets - short haul. 3- OnTrack2 is sold to all segments of the transportation industry including fuel and hazardous material industries.4- There is a $595 hardware charge. 5- The base monthly service fee is $25 a month, and a separate wireless fee from $15-20.

	Possible Applications																									Current Operations			Pricing				
Company	Satellite Tracking	Cellular Phones or Paging Service	Terrestrial Tracking	Automated Collision Notification	Trailer Tracking	Untethered Trailer Tracking	Keypad Personnel Authentication	Trailer Securement	Biometric Authentication	Driver Authentication	Asset Management	Asset Tracking	Mapping	Remote Vehicle Disabling	Inventory Management	Web-based Shipment Tracking	Radio Frequency Identification Tag	Out of Route Mapping System or Ale	Electronic Cargo Seals	Mechanical Cargo Seals	In-Vehicle Mounted Computer	In-Vehicle Communications	Integration Software	Consultant Services	Others, please describe	Average Operation Size	Type of Operation	Market Expansion	Per Unit Base Cost	Per Unit + Installation	Maintenance Costs	Recurring Service Costs	Notes
TrackStar	X	X	X				X		X	X	X	X	X	X	X	X	X	X			X	X	X	X	X - (see note 1)	See Note 2	See Note 3		See Note 4			See note 5	1- systems integration; peripheral integration; web-services; custom solutions; corporate unlimited-use license. 2- Track Star has had success with many different carriers, but has seen small to medium-sized carriers the most. 2- Operations ranging from hazmat, armored vehicles, executive protection and many carriers in Latin America. 3- Operations ranging from hazmat, armored vehicles, executive protection and many carriers in Latin America. 4- There is a $995 hardware cost and a $295 seat license fee. 5- It costs approximately $30-35 a month for the terrestrial cell fee per unit.
Transcore			X	X									X					X														
Trimble																										See Note 1	See Note 2		See Note 3				1- Operation size varies greatly. 2- They provide services for ready mix and construction as well as fleet-based carrier companies. 3- The product can range from $550 to $3,000 based on the customization of added sensors.
Vericom Technologies									X	X				X																		
Vistar	X		X										X																			
Waveburst Communications, Inc.																																
Xata																																
Aeris.net																																
PowerLoc Technologies, Inc.																																
V-TRAC Systems, INC																																

Appendix D.
Beta Test

Introduction

The Beta Test summary provides detailed information on the Beta Test that took place in July of 2003 at Qualcomm Headquarters in San Diego. The purpose of the Beta Test was to test the functionality of each technology individually as well as in concert with one another. In addition, it provided both the Deployment and Evaluation teams with a chance to view the data streams and adjust collection process accordingly. The Beta Test Addendum outlines those configuration changes that were identified during the Beta Test. The Beta Test of the FOT was performed on July 14-18, 2003 and utilized the Qualcomm technology truck and included members of the Deployment Team and the Independent Evaluation Team.

D.1 Objective

There were two primary Beta Test objectives. The first was to ensure that selected test technologies perform adequately in simulated scenario conditions. The second objective was to ensure that generated test data streams fulfilled requirements to allow for thorough Independent Evaluation analysis.

D.2 Process

The Beta Test focused specifically on Scenario 1 – Bulk Fuel, and Scenario 4 – Truckload Explosives. These Scenarios were chosen as they represented the full continuum of FOT technologies and it was recognized that if their functionality met test conditions, it was generally unnecessary to pre-test the other scenarios. For the purpose of the Beta Test, Scenarios 2 and 3 were treated as subsets.

Scenario testing was broken into 3 functional components: (1) system configuration, (2) daily operations/processes, and (3) security breaches. A detailed script was developed for each scenario. The following are Scenario 1 and 4 overviews.

D.2.1 Scenario 1 – Bulk Fuel

- Scenario Participants: 1A – Dupre Transport LLC; 1B – Cox Petroleum
- 25 trucks
- HazMat: Class 3 (Flammable Liquids)
- Platform: QTRACS/400 and QT Brazil
- Technologies Tested:
  - Wireless Satellite/Terrestrial Communications
  - In-Dash Panic Button with Notification
  - Global Login
  - OBC with Remote Disabling

- OBC with Loss of Signal Disabling
- OmniOne Digital Phone
- Wireless Panic Button with Local Disabling

D.2.2 Scenario 4 – Truckload Explosives

- Carrier Participant: 4A – R&R Trucking; 4B – Dyno
- 25 Trucks
- Hazmat: Class1.1-1.6 (Explosives)
- Platform: QTRACS/Web; Saflink Web; QT/Brazil
- Technologies Tested:
  - Wireless Satellite Communications
  - Dash Panic Button with Notification
  - Wireless Panic Button with Local Disabling and Notification
  - Biometric Verification
  - ESCM
  - OBC with Remote Disabling and Loss of Signal Disabling
  - Geofenced Mapping
  - OBC with Trailer Door Lock System
  - Electronic Cargo Seals
  - Untethered and Tethered Trailer Tracking

Each detailed Scenario script went through a "day in the life of" a driver and their possible route (Figure D-1). The technology truck was equipped with a switch box which allowed all technologies to be connected at once and, based on the scenario, the appropriate switches turned on. The Beta Test was operated from one of the vendor headquarters, so the shipper and consignee roles were simulated using a laptop computer and defining locations such as a rest area as the consignee.

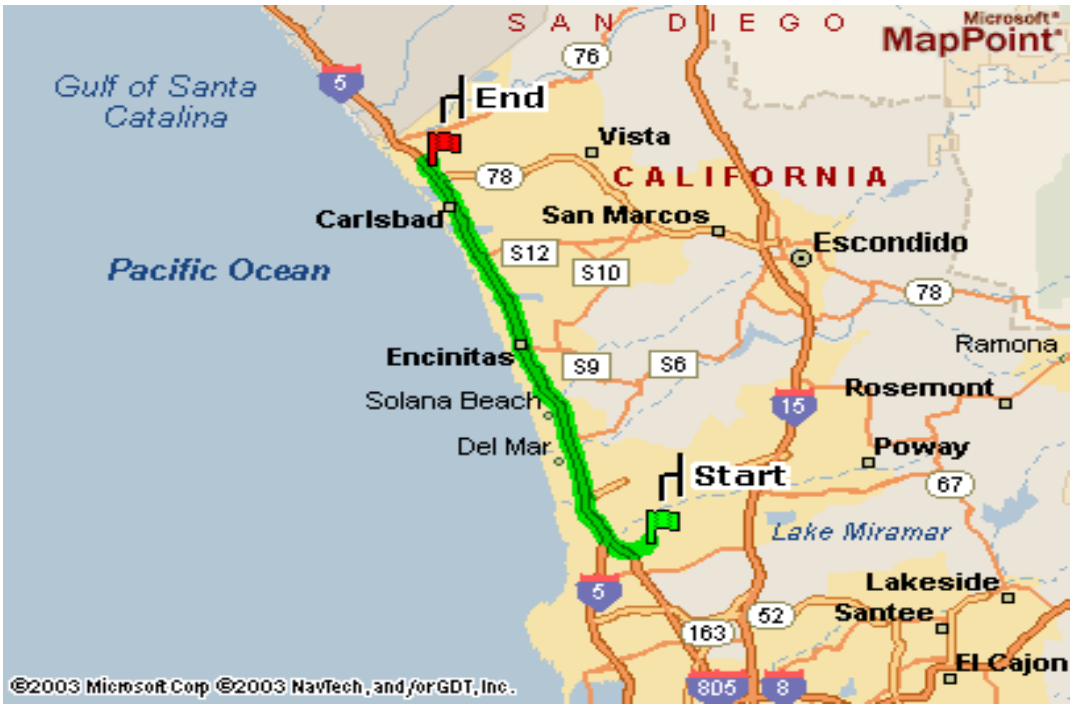

Figure D-1. Beta Test Route

Each segment of the detailed test script was tested and its performance documented. Throughout the Beta Test, the teams identified several possible configuration changes. Those will be noted in the Section D.3. Figure D-2 shows a screenshot depicting Global Login in which the driver has logged on/off.

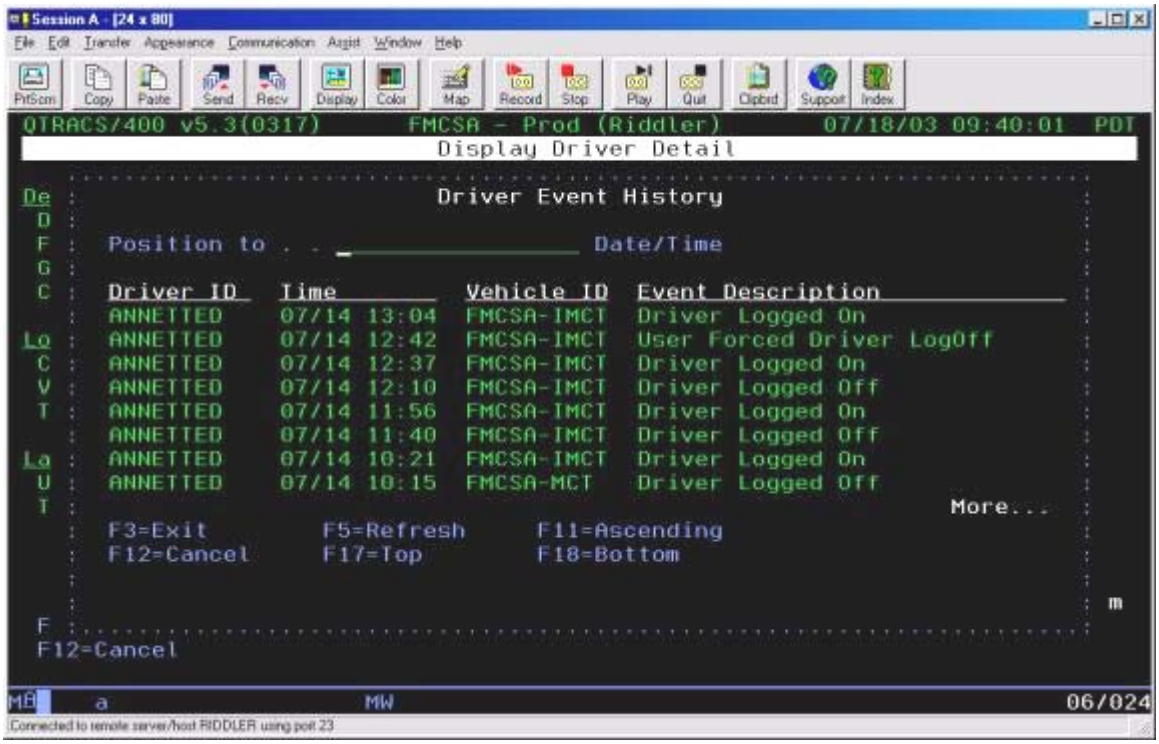

Figure D-2. Global Login Data

The last day of the Beta Test, the Deployment and Evaluation Teams went through the data streams generated by the test to ensure that the data would be presented in a digestible format. Category headings were changed and some data fields were deleted.

Using the feedback and performance issues for each of the technologies during the Beta Test, several configuration improvements were identified.

- The 'OBC with loss of signal disabling' was re-configured to activate throttle disable while vehicle is driving >20 mph.
- The 'OBC with trailer door lock' was reconfigured to allow a driver 60 seconds from the time the button is pushed to the trailer door automatically re-locking.
- The Savi software will incorporate an e-mail notification to carriers of seal status changes.
- Differentiation of color coding for Savi website events was made.
- Investigation of the placement of the seal on a trailer door in order for the antennae to be read was performed.

A presentation was made to the Hazmat Working Group via WebEx of Beta Test process and the configuration changes. After the changes were agreed on by all, an Addendum to the Detailed Test Plans document was prepared and can be found in the next section.

D.3 Beta Test System Design Addendum

*System design changes are highlighted throughout the table.

Technology	Function	Pass	Fail	Revisions Needed
Wireless Satellite Communications (w/ GPS and/or QASPER)	Utilizes satellites to link and log all system technologies from vehicle to the communications system.	X		
Wireless Terrestrial (w/ GPS and/or Cellular)	Utilizes cellular communications to link and log all system technologies from vehicle to the communications system.	X		
OmniOne Digital Phone	Host creates and sends a load assignment to driver w/ OmniOne phone.	X		
	Driver and host exchange five different macros based on situation, i.e., unload/load, departing, stop.	X		
Dash Panic Button w/ Notification	Driver depresses the wired panic button and a “panic message” is sent to NMC from mobile unit.	X		
	NMC forwards “panic message” to carrier.	X		
	“Panic message” is copied to Law Enforcement via QMASS.	X		
	NMC personnel call to notify carrier of emergency situation. Call received w/ vehicle identification number.	X		
Wireless Panic Button w/ Notification	Driver depresses red panic button on wireless panic button transmitter.			
	Wireless panic button transmitter sends “panic message” signal to mobile unit, which in turn sends message to NMC. Host receives panic message.	X		
	NMC forwards message to carrier, as well as calls carrier and law enforcement (in some scenarios) with vehicle identification number.	X		
	Law enforcement account, QT/Web 3.1, is copied with panic messages and positions of truck.	X		

Technology	Function	Pass	Fail	Revisions Needed
Wireless/Local Disabling	Attached to wireless panic button w/ notification, although driver disables vehicle by pressing separate Aux button on wireless panic button transmitter.	X		
	Wireless panic button transmitter sends a command to disable vehicle; throttle is disabled.	X		Long Term Consideration: Develop notification for local disabling
	Driver depresses reset button on wireless panic button transmitter; throttle reverts to normal.	X		
Global Login	Logon	X		
	Logoff	X		
	Communications between NMC and MCT validating driver logon.	X		
	Driver hears audible warning and gets a message prompting him to logon every two minutes.	X		
	Driver starts engine but does not logon. After five minutes of idling a Global Logon security breach is sent to the Carrier.	X		
	Driver starts engine and departs without logging on. After driving one mile a Global Login security breach is sent to the Carrier.	X		
	Driver logs into mobile three times unsuccessfully, and security breach is sent to the Carrier.	X		
	Host dispatcher logs off driver.	X		

Technology	Function	Pass	Fail	Revisions Needed
Biometrics Login	Driver inserts smart card into slot on biometric device; driver places finger on scanner for verification; when verified green LED blinks.	X		
	Message containing driver's global login user name and password to NMC for verification; NMC sends notification to carrier. Driver ID is displayed next to vehicle name.	X		
	Driver starts engine and does not log on via biometrics. An audible beep is generated after two minutes to prompt driver to logon. After five minutes or one mile driven with no logon, a Global Login security breach is sent to the Carrier.	X		
ESCM	Shipper logs onto ESCM w/ fingerprint and smart card and creates electronic manifest.	X		
	An e-mail is generated to inform the carrier and consignee of manifest ID; carrier notifies driver.	X		
	Driver departs for shipper; at shipper, driver logs on to ESCM system and logs on to accept responsibility for specific load/manifest. E-mail notifications sent to carrier and consignee.	X		
	Driver departs for consignee; at consignee, he logs on to ESCM system and transfers responsibility of load/manifest to consignee. E-mail notifications sent to carrier, consignee and shipper.	X		
OBC w/ Remote Vehicle Disabling	Carrier sends an over-the-air message to the OBC disabling the vehicle.	X		
	Verify that after message is sent, throttle is disabled.	X		
	Carrier sends over-the-air message to OBC enabling the vehicle.	X		
	Throttle is enabled.	X		

Technology	Function	Pass	Fail	Revisions Needed
OBC w/ Loss of Signal Disabling	OBC monitors the communication system for a loss of signal; recognizes loss of signal.	X		
	OBC identifies loss-of-signal for seven minutes while vehicle is driving >35 mph and activates throttle disable. Host sees Signal Loss Alert.			'OBC with loss of signal disabling' will be re-configured to activate throttle disable while vehicle is driving >20 mph. Seven minute threshold remains the same.
OBC w/ Trailer Door Lock System	Driver sends an over-the-air message to host requesting trailer door unlocked; host receives "unlock trailer macro."	X		
	Driver presses trailer door switch in cab and then has 20 seconds to walk back to open the door, or door will default to lock.			OBC w/ trailer door lock system will be re-configured to allow driver 60 seconds from time button is pushed to trailer door opening.
	If door lock is tampered with, an alert is sent to the mobile, which in turn sends an alert event to NMC and then Carrier.	X		
Electronic Cargo Seals	Driver logs onto the TSS system and uses mobile reader to collect the S/N of the e-seal in range; seals are bolted, and driver notes S/N of e-seal.	X		
	Driver sends an over-the-air command to assign and seal each seal separately.			Extremely time consuming to assign and seal each separately. It may be possible for this to occur all at once. It is also very hard to view information on the handheld.
	Carrier is able to view sealed locks on website.			Screen has to be constantly refreshed to see updates. New SAVI software will incorporate e-mail notification to carriers.
	Driver enters mobile reader into surveillance mode for assigned seals.	X		
	When a seal is tampered with, an alert is sent to the carrier, and an audible alarm sounds.			Differentiation must be made between red and black type for events logged on the SAVI website.
	If a seal becomes undetected, and alert is sent to the carrier and an audible alarm sounds.			Investigation must be made into the placement of seal on door in order for antennae to be read.

Technology	Function	Pass	Fail	Revisions Needed
Geofenced Mapping	Carrier initiates a route-based geofence trip on a designated route.	X		
	Once trip is initiated, 15 minute position requests are made to the unit by the host system.	X		
	Carrier monitors vehicle for positions and is able to view on a route map.	X		
	When driver deviates from the designated route over ½ mile, the host system begins requesting positions every five minutes.	X		
	As driver enters geofenced area, the host system begins requesting positions every 3 minutes.	X		
Tethered Trailer Tracking	Driver hooks tractor to trailer, tethered trailer unit transmits the tethered trailer track ID over power bus to the mobile unit. Trailer ID displayed on unit.	X		
	Mobile unit sends and over-the-air message to carrier to notify them of connect event. Connect message is displayed on TT/Win.	X		
	Driver unhooks the tractor in consignees yard, mobile unit detects lack of trailer tracks ID and sends over-the-air disconnect event to carrier.	X		
Untethered Trailer Tracking	When trailer is disconnected the Carrier creates a rectangular geofence around trailer, and GT unit verifies hourly that it has not left that area.	X		
	If it is taken from geofenced area an alert is sent to carrier, and position reports can be configured to be sent frequently.	X		
QTRACS/400	Computer system/server for satellite and terrestrial communications.	X		
QTRACS/Web	Computer system/server for satellite and terrestrial communications.	X		
QTRACS/Win	Computer system/server for satellite and terrestrial communications.	X		

Technology	Function	Pass	Fail	Revisions Needed
SAFLINK Web	Computer system/server for biometrics and ESCM.	X		
SAVI Web	Computer system/server for electronic cargo seals.	X		
QT/Brazil	Computer system/server that controls remote vehicle shut down and trailer lock/unlock.	X		
GT/Web	Computer system/server that monitors untethered trailer status.	X		
TT/Win	Computer system/server that monitors tethered trailer status.	X		

NOTICE: This document has been approved for public disclosure. Appendix E containing Sensitive Security Information has been removed. References to this appendix remain in the document.

Appendix E.
Sensitive Security Information